

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

FEDERAL TRADE COMMISSION

WORKSHOP :

PARTNERSHIPS AGAINST CROSS-BORDER FRAUD

THURSDAY, FEBRUARY 20, 2003

FEDERAL TRADE COMMISSION
6TH AND PENNSYLVANIA AVENUE, N.W.
WASHINGTON, D.C.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

	PAGE:
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	

TABLE OF CONTENTS

OPENING REMARKS

Commissioner Mozelle W. Thompson 3

PANEL 5: COOPERATING WITH COMMERCIAL MAIL
RECEIVING AGENCIES AND COURIER
SERVICES 5

PANEL 6: THE ROLE OF INDUSTRY ASSOCIATIONS
AND SELF-REGULATORY ORGANIZATIONS 49

REMARKS INTRODUCING INTERNET-RELATED PANELS 80

PANEL 7: POTENTIAL PARTNERSHIPS AMONG CONSUMER
PROTECTION ENFORCEMENT AGENCIES AND
INTERNET SERVICE PROVIDERS AND WEB
HOSTING COMPANIES 85

PANEL 8: COOPERATION BETWEEN CONSUMER
PROTECTION ENFORCEMENT AGENCIES AND
DOMAIN REGISTRATION AUTHORITIES 139

CONCLUDING REMARKS: J. HOWARD BEALES, III 250

P R O C E E D I N G S

- - - - -

1
2
3 MR. STEVENSON: We're ready to get started. We
4 seem to have lost one panelist in the snow. We are
5 going to proceed ahead.

6 COMMISSIONER THOMPSON: It's a conspiracy. If
7 we don't like you, we lose you in the snow.

8 Good morning, you all. Thank you very much for
9 coming to the FTC for our second day on our partnerships
10 against cross-border fraud workshop. Now, I know there
11 are a lot of you who have come from very long distances
12 to be here and participate. I'm specifically mentioning
13 our folks from the customs service and -- no, some of
14 our foreign guests from Australia and the UK and, yes,
15 even Canada, where they think the snow that we've had is
16 just like a little blip.

17 Well, thank you very much for coming. Now,
18 yesterday, we heard some very interesting discussion,
19 especially about cross-border fraud trends in the
20 financial services industry, and heard a little bit
21 about the experiences in financial services in
22 combatting cross-border fraud. Today, we're going to
23 hear some other interesting information from people who
24 are involved with commercial mail, people involved in
25 industry self-regulation and in the more high-tech

1 industries of the Internet. We'll also hear after lunch
2 from the domain registration authorities, one I'm
3 particularly interested in.

4 So, now, yesterday I talked a little bit about
5 some of the real opportunities that we have here in
6 combatting cross-border fraud, but also the recognition
7 that neither government nor businesses, nor consumers,
8 alone, could find solutions to fraud that takes place on
9 a global basis. It's an opportunity for us to set aside
10 our usual suspicions about how different branches of the
11 world operate and to recognize in order to set the right
12 course for the future, and that future is something we
13 all have an interest in, that we have to work more
14 cooperatively and to recognize that each of us have a
15 role in shaping what future policy is.

16 So, I'm not going to delay too long, because I
17 know that we want to get to the panels, and to hear what
18 they have to say. So, on that note, I welcome you all
19 here, and I again want to give a special thanks to the
20 staff who put this together, the folks in the
21 International Consumer Protection, who have worked
22 really hard to arrange the snow, and everybody who has
23 especially brought materials here and left it out on the
24 table in hopes that they won't have to carry them home.

25 So, thank you very much for coming. And, now,

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

1 there's just one point that I do want to raise as part
2 of my prerogative, is this: I would like to see this as
3 a starting point and not an ending point. I think that
4 we've spent a long time, each of us, working in our
5 various fields talking about, gee, wouldn't it be nice
6 if we found more formal ways of cooperating with each
7 other to solve these problems.

8 It is my hope, whether it's on a one-on-one
9 basis by the people sitting in this room, or by looking
10 at the categories of subjects that we've talked about
11 today and tomorrow, yesterday and today, that we can sit
12 down and have a more formal relationship, and hopefully,
13 perhaps, have more of these workshops, either here
14 sponsored by the FTC, or outside of the FTC where we can
15 work on solutions and identifying new problems as they
16 arise.

17 So, that's the challenge that I have for all of
18 you, to make this last beyond what we've gone through in
19 two days, but to make it more meaningful for consumers
20 and businesses, and, yes, even us in government, because
21 we're here to help you. Thank you very much.

22 MS. FEUER: Great, I would like to get started
23 now with our first panel, so if the panelists can come
24 up and take their seats by their placards, that would be
25 great.

1 Before we get started, I just want to apologize
2 for leaving my cell phone on. We are missing one
3 panelist, Charmaine Fennie, who I believe is traveling
4 on the red eye from Seattle. So, unfortunately, we are
5 going to get started without her, and there is a gap,
6 but if my cell phone rings, I apologize, because I left
7 my number for her to call.

8 So, with that, good morning, I'm Stacy Feuer,
9 Legal Advisor for International Consumer Protection here
10 at the FTC. During the last panel yesterday, we focused
11 on payment systems, a type of legitimate business, or I
12 should say businesses that are often used by
13 cross-border fraud operators to facilitate frauds,
14 mainly to get money from victims. Today we're going to
15 look at two other types of legitimate businesses that
16 are often used by fraud operators for the same purposes,
17 as well as for other incidental matters in fraud
18 schemes.

19 To discuss this, I am pleased to welcome, and
20 I'll do this alphabetically, so if you want to just
21 raise your hand, Alan Armstrong, who is a long-time
22 major franchisee for MailBoxes Etc., and he is
23 responsible for the Washington metropolitan area. He is
24 here representing MBE, both at the regional and
25 corporate level.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

1 Also, Lee Hollis, who is the General Manager for
2 Enforcement Coordination at the Australian Competition
3 and Consumer Commission. Robin Landis, next to me, the
4 Program Manager for Telemarketing Fraud with the U.S.
5 Customs Service. He recently returned to DC after
6 working with our law enforcement counterparts across the
7 border for the past year or so, through Project Colt in
8 Montreal.

9 Larry Maxwell -- sorry, I skipped Andy Lynn,
10 Director of Marketing and International Property Law at
11 FedEx. In that capacity, Andy works with the security,
12 revenue and IT units at FedEx to detect and prevent
13 fraudulent transactions. And last but not least, Larry
14 Maxwell, the Inspector in Charge of the Fraud, Child
15 Exploitation, and Asset Forfeiture Group for the Postal
16 Inspection Service.

17 What I would like to do with this panel, as we
18 did yesterday afternoon, is throw out a few questions,
19 first about opening matters such as current issues and
20 trends affecting the use of CMRAs and courier services
21 in the cross-border fraud arena, and then halfway
22 through, move on to possible mechanisms for enhanced
23 cooperation between law enforcement agencies, including
24 the three of us who are sitting here, Customs, the U.S.
25 Postal Inspection Service and the FTC, and the private

1 sector.

2 What I would like to do is keep this discussion
3 interactive. So, while I'll address some of my
4 questions to particular panelists, if you want to
5 respond and weigh in on somebody's comments or a
6 question I have asked, just raise your table tent and I
7 will recognize you.

8 So, I am going to start with Robin, since he is
9 sitting right next to me, and ask, what are the main
10 challenges you see for law enforcement arising out of
11 the use of commercial receiving mail agencies and
12 courier services in fraudulent cross-border
13 telemarketing schemes?

14 MR. LANDIS: Well, thank you, Stacy, I
15 appreciate coming here to talk to you about
16 telemarketing fraud.

17 The U.S. Customs Service believes that
18 telemarketing fraud is a big problem. I spent three
19 years up in Montreal just doing telemarketing, and we
20 just opened an office with three agents working in
21 Montreal, Toronto, and Vancouver that's trying to
22 address this problem. And I would like to kind of
23 explain to you how it really works.

24 Now, would you be surprised if I told you that
25 telemarketing out of Canada is organized crime? It's

1 organized crime. It is organized crime. The proceeds
2 that they're receiving from this telemarketing fraud,
3 and we estimate just in Montreal alone is \$200 million,
4 just Montreal. These proceeds are being used to buy
5 narcotics, to fund drug operations, the smuggling of
6 guns, and prostitution. We have documented this. It is
7 organized crime.

8 It's set up basically in a four-part
9 organization. They have a leader, a captain, and they
10 have lieutenants. How is it broken down? Well, you
11 have a lieutenant that's in charge of leads. Leads are
12 the victims' telephone numbers. That is very, very
13 sought after. You have another lieutenant who is in
14 charge of the boiler rooms, or the telemarketers. When
15 I say boiler rooms, you probably think of a room that
16 they rent in a business, it's not that anymore. It
17 could be five, six, seven people sitting in cars in a
18 parking lot of a mall with cell phones, calling the
19 victims with their lead sheets. Or it could be a hotel
20 room where they rent it for 24 hours. They move very
21 fast.

22 So, the boiler room has really changed to a
23 mobile location. It's all in charge by one individual,
24 a lieutenant.

25 The third lieutenant would be in charge of the

1 money laundering. You have the leads, the
2 telemarketers, then they have to get the money. So,
3 they have a person in charge of nothing but pertaining
4 to money.

5 And a fourth lieutenant who is in charge of
6 security. And what I mean by security, they enforce and
7 keep the organization together. They do not want the
8 telemarketers to steal any of the leads, they want to
9 make sure that the leads are brought in timely, and it
10 just keeps the organization together. Most of the
11 security people are street gang members. Very violent.

12 How do we attack this? We want to attack it by
13 prevention, disruption, and prosecution. When I talk to
14 you about leads, that is probably the most important
15 thing that they look at. Every search warrant that
16 we've done in Montreal, we always found the original
17 leads sheets. A lead sheet is a mailing of a
18 sweepstakes somewhere to somebody in the United States
19 asking them to enter a contest and put their phone
20 number on it. We are finding the original sweepstakes
21 in Montreal from these telemarketers. They're either
22 mailed from outside the United States or within the
23 United States to the victims who respond.

24 How do we prevent this? Well, we have executed
25 some search warrants in the United States to go after

1 the leads brokers. The sweepstakes entries. We want to
2 prevent it because we think that's the key to the
3 telemarketers. If they don't have the phone numbers,
4 they're not going to call the victims. We want to
5 prevent the person of responding to the calls, so
6 prevent the mailings, prevent the telephone calls, and
7 then prevent the victim from sending the money. That's
8 our prevention strategy in telemarketing.

9 Disruption: What I mean by disruption, we want
10 to seize the mailings, shut down the phone lines, or
11 seize the money coming from the United States to the
12 foreign country.

13 In one case that I worked starting in '92, one
14 telemarketing organization out of Canada had three
15 boiler rooms. Their telephone bill was over \$1 million
16 a month with 1,000 telemarketers calling to the United
17 States seven days a week, 16 hours a day. In the
18 indictment we had, we documented \$118 million in one
19 year.

20 We're also shutting down phone lines and we're
21 also seizing mail that's coming into or going out of the
22 United States. We're also conducting a lot of
23 prosecutions lately, with the U.S. Attorney's Office
24 from mailers, printers, who are aiding and abetting,
25 knowingly. The telemarketers that are doing the

1 telephone calls in Canada, and elsewhere, and also the
2 money launderers, which include money transmitters,
3 bank-to-bank wire transfers, and also individuals who
4 are operating drop sites.

5 Working with the mail receivers or the express
6 couriers, last year, just in Montreal, we intercepted
7 and seized over \$1 million cash going to telemarketers
8 in Montreal. Under our program, we seize it, we return
9 the money back to the individuals. U.S. Customs
10 agents actually go to the victim in the United
11 States, return the money to them, and interview them to
12 see why they were victimized, what was the statements
13 made to them, what were the promises, and why they sent
14 it.

15 Just one year operation in Montreal, we have
16 documented over 1,500 drop sites where mail is going to
17 them from telemarketers.

18 MS. FEUER: Robin, thank you. So, yesterday we
19 talked about money going to a wire transfer through a
20 debit card through ACH Debits, but what you're saying to
21 me it sounds like Customs Service is still seizing lots
22 of money that the victims are sending that is making
23 its way from the victims' pockets to the telemarketers
24 by the mail and express mailing couriers.

25 MR. LANDIS: Correct. A lot of it is cash, a

1 lot of it is cashier's checks.

2 MS. FEUER: And that's interesting, because it
3 does seem consistent with some of the new statistics
4 that we're releasing that checks are still a big payment
5 method in these schemes.

6 I'm wondering, Larry, whether you're seeing the
7 same types of things, and if you could focus in part on
8 obviously the Postal Inspection Service viewpoint how
9 CMRAs are used and what kinds of trends you're seeing in
10 connection with telemarketing fraud and Internet fraud
11 as well.

12 MR. MAXWELL: Sure. First, Stacy, I just want
13 to thank the Commissioner and FTC for hosting us and
14 inviting me and my agency and our friends here from the
15 other agencies.

16 Everything Robin just mentioned is dead on
17 point, accurate. As he said, he spent time up in
18 Montreal. We have an inspector assigned to Montreal and
19 we are exploring expanding our role up there. We've
20 been up there for several years now. We also have an
21 inspector, two inspectors assigned to the Partnership
22 Alliance in Toronto with FTC, and we're starting a new
23 operation now out in Vancouver and the western part of
24 the country.

25 As Robin mentioned, organized crime is a real

1 factor in Montreal, and telemarketing is the big focus
2 there for us. If you go to Toronto, one of our biggest
3 concerns there has been the advanced fee schemes, but
4 there's a variety of other types of frauds we do see.
5 You get out west, of great concern to me, being a
6 representative of the Postal Service here, is the
7 lottery, we have a preponderance of lottery schemes
8 coming in. I hear this from the Canadian authorities
9 and I hear this from consumer agencies, I hear this from
10 FTC and Department of Justice.

11 So, we kind of have a little different hydra, if
12 you will, in terms of the types of crimes, in terms of
13 the use of commercial mail receiving agencies. I left a
14 brochure out -- it's not a brochure, it's a couple of
15 pages that the Postal Service and the Inspection Service
16 put out a few years ago when we enhanced our regulatory
17 provisions guiding commercial mail receiving agencies.
18 And essentially, it lays out the facts for you and it's
19 pretty current.

20 There are a few modifications that it doesn't
21 mention that I can clarify later if you have any
22 questions, but primarily, what we did was, and this goes
23 in a chapter No Good Deed Goes Unpunished. We heard for
24 years from law enforcement, both in Canada and here in
25 the States, that commercial mail receiving agencies were

1 becoming a haven for criminals. Well, we only had
2 anecdotal information. We only had agents telling us
3 this. None of our databases captured this information,
4 ours or others.

5 But we tried to proceed in enforcing new
6 regulations and met with a very logical reaction from
7 the industry. You know, you're basically taking a
8 shotgun to a canary here. And we looked at it and
9 decided the best course was to meet with them and work
10 out reasonable accommodations that fit both sides.

11 We recognized we couldn't force feed our
12 thoughts on anyone based on no empirical data to back us
13 up. So, we agreed to modify our data mechanisms to
14 capture those statistics so we would have a better clue
15 and also provide some intelligence for future
16 investigations and trend analysis. But lacking that, we
17 worked on what I would call a common sense parameter.

18 Oftentimes in telemarketing schemes, both within
19 the States, for instance in New York, where I get my
20 experience from, you would have boiler rooms operating
21 very temporarily, using phones, and they would use
22 commercial mail receiving drops. Sometimes they would
23 even use a post office box, but post office boxes had a
24 little more direct contact with the Post Office, so
25 there was a reluctance to use that on their part.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

1 They could use pretty much anything to describe
2 the address, as many of you probably are very familiar
3 with, you could use suite 24, and to a potential victim
4 customer, could look at that and say it sounds like a
5 legitimate concern and mail it off thinking it goes to a
6 nice corporate building somewhere, where in reality it
7 went to a small mail drop place and the person would
8 come in in anonymity, sometimes sending someone else
9 down to pick it up.

10 There were requirements on the books that
11 frankly the Postal Service didn't do a good job at
12 enforcing at this time, and that was a form required.
13 It's an application for delivery of mail through an
14 agent. It's a 1583, so we will feel comfortable with
15 government forms. There's two forms. There's one form
16 the CMRA operator fills out which authorizes them to be
17 a CMRA, and that's a little bit more comprehensive in
18 terms of information required.

19 The second, which is the CMRA boxholder, fills
20 out an application the same way. What we did in the new
21 regulations, just in a nutshell is we enhanced the
22 identification requirements and the validation of those
23 requirements. So, the postmaster validates the CMRA,
24 the CMRA owner/operator would validate their customers.
25 And on a quarterly basis, provides that information to

1 local post offices, the current list. So, we have a
2 listing of actually who we deliver mail to.

3 Does the Postal Service compile lists of private
4 information, social security number, addresses? No, we
5 do not. And as a law enforcement officer, I would love
6 to have that information, because it would make my job a
7 lot easier, but in a democracy, there are groups that
8 feel that's an intrusion of privacy, and we have to
9 respect that.

10 I was part of a side working group dealing with
11 the abused spouse organizations, and they had some major
12 concerns about releasing this information, even to law
13 enforcement, without court orders. So, we restricted a
14 lot of that information based on our recognition that
15 there are people who could get hurt in this process for
16 us. So, that is a big obstacle we have faced.

17 We have mechanisms in place now which appear to
18 be working. Recently, I ran the statistics, which does
19 not show a dramatic usage of CMRAs to my surprise, but
20 part of that comes, it's like the chicken and the egg.
21 I mean, we implemented these new regulations, which
22 eliminated mailers from using terms like suite or some
23 other designation for an office, and they had to use two
24 designations, they had to use either the term PMB, for
25 private mailbox, similar to post office box, and that

1 seemed like a good catch, we had a nice comparison.
2 However, some people did push back on that, and they
3 felt they wanted one other alternative, because they
4 felt PMB was too restrictive.

5 And, again, you're dealing with a lot of
6 legitimate businesses that have needs and want to change
7 and have image and branding and so forth. So, we gave
8 them the pound sign, the numeric pound sign symbol, they
9 could use that, or PMB. And that may have, for those
10 honest operators out there, those mailers, that may have
11 decreased some of the use of the CMRAs, in the United
12 States.

13 There are commercial mail receiving agencies, of
14 course, around the globe. We have worked, as I'm sure
15 Robin has, and others here, with Canadian counterparts.
16 And just like you would a victim on the street or a
17 witness on the street, some are very cooperative and
18 helpful, even when they don't have to be, and then
19 others basically tell us to take a hike.

20 So, we have no legal jurisdiction to enforce
21 them. The Canada Post Institution, which is the U.S.
22 Postal Service counterpart, they do not have
23 requirements on registering commercial mail receiving
24 agencies, to my knowledge, unless that's changed very
25 recently, and I don't believe it has.

1 Again, I don't know if their thinking is to
2 enforce such regulatory change up there, but I think
3 they saw what we went through and probably thought
4 better of it. But they may at some point. And I think
5 it is good to know your customer, who you deliver to,
6 and it protects a lot of people, and it protects the
7 Post Office. We deliver to a lot of people. And that
8 creates another major obstacle.

9 Again, this information is private information,
10 people like to protect their identity, they do like to
11 protect their personal privacy for a lot of reasons.
12 And in some instances are very open out there. But we
13 have to respect both parties. So, that does present a
14 challenge.

15 My concern goes even further in dealing with the
16 cross-border issue. It's been a great opportunity for
17 U.S. law enforcement and Canadian law enforcement to
18 work together to iron out a lot of these kinks that come
19 from two very friendly nations that speak mostly the
20 same language and share a lot of the same institutions
21 and laws. What's happening is, as all of you are aware,
22 and it's a big focus of Hugh Stevenson and his group,
23 is the emergence of international fraud and crimes and
24 how we are going to deal with that in the coming
25 decades.

1 That's a concern. I mean, over the years, we've
2 had trouble keeping the genie in the bottle on our own
3 domestic crimes and now we're looking at victimization
4 from outside our parameters. And I think using the data
5 and intelligence is a great asset for us. If we can
6 show trends. For example, very clearly, we're seeing
7 most of the victims coming from the lottery schemes and
8 the operations coming from western Canada, are in the
9 Southern California/Arizona area. It pops out at you on
10 a map when you run some of that data and it's very
11 helpful to use FTC data or our own data, data provided
12 by the Canadians. And that's helpful.

13 MS. FEUER: Thanks. And, Larry,
14 one follow-up question before we move on. It's good to
15 hear that CMRAs are being used less in these schemes.
16 I'm wondering, though, about the phenomenon that we
17 sometimes hear in our investigations is somebody using a
18 U.S. address at a commercial mail receiving agency and
19 then having that mail forwarded on to Canada or some
20 other place. Does your data pick any of that up?

21 MR. MAXWELL: No, that is a lacking portion.
22 What happens is the Postal Service, although now I think
23 we're much better off in our working relationships with
24 the commercial mail receiving agency industry. We have
25 a lot more contacts, there's a lot more communication,

1 if you will. And as I said, the vast majority are
2 legitimate users of that service and it's a very
3 valuable service. However, we do not regulate. We can
4 regulate our requirements to deliver mail to that
5 agency, but we can't regulate the users and we can't
6 regulate the industry and what they choose to do.

7 MS. FEUER: Right.

8 MR. MAXWELL: So they can forward it on. We
9 can't require records of that. Our hope there is
10 cooperation from the agency manager that maybe would
11 alert us to some kind of suspicion. Again, you know,
12 it's sort of a dichotomy there, because they have
13 customers, they want to preserve their privacy.

14 We also rely on Customs, our Customs, Canadian
15 Customs. I'm looking at ways now, it's interesting, you
16 were talking about forwarding the mail out, Robin was
17 talking about a conversation we had earlier, too, was
18 what interests me is that to get around the border
19 search now, what they do is mail into the United States
20 or actually have the printing done in the United States.
21 Robin mentioned that they shut down some printers.
22 That's probably one of the better strategies right now
23 to use is to look at what's happening here in the United
24 States that we can control.

25 You know, are they printing, producing, mailing,

1 distributing here? If they're forwarding it, that's a
2 different animal there.

3 MS. FEUER: Right. Let me turn to Alan
4 Armstrong, who is --

5 MR. ARMSTRONG: Do I get my chance now?

6 MS. FEUER: Yes, he was our lone CMRA
7 representative because unfortunately Charmaine Fennie
8 has not made it. But, Alan, let me ask you the
9 flip side, because you and I have talked about the fact
10 that CMRAs are used for a variety of scams, including
11 consumer scams, but we talked a little bit about what's
12 being done by MBE in that area. So, if you could
13 expound on that for us.

14 MR. ARMSTRONG: I mean, there was a lot of
15 things that were covered by Larry, and I know that --
16 and I agree with a tremendous amount of them. I think I
17 would like to say to begin with that cooperation,
18 particularly at the local level, between our individual
19 stores and centers, and I don't mean to speak for the
20 entire industry, I can speak for MBE, but I think I'm
21 pretty comfortable in saying that it's this way with the
22 other franchises and also with the independents that
23 Charmaine represents.

24 Going at it another way, I think at the local
25 level to work with the Postal Service, the Secret

1 Service, the FBI, and God knows how many other people we
2 see kind of come into our facilities over the years.

3 I just want to say that those of you who read my
4 background, I'm an area franchisee from MailBoxes Etc.,
5 but 17 years ago when I got started with MailBoxes Etc.,
6 I was an individual store owner and I had a couple of
7 stores. So, I kind of lived all this, and the customers
8 coming in and the problems and the concerns and dealing
9 with the Postal Service and all these other folks. And
10 it's been a lot of change over the years. And I think
11 we've learned an awful lot about each other and how we
12 can work together.

13 So, I think there has been a lot in that regard.
14 I would mention that there are sometimes conflicting
15 regulations as it relates to the pressures on the
16 individual CMRA in terms of trying to work with the
17 authorities, whether they be the Postal Service or the
18 FBI, the Secret Service, in terms of trying to want to
19 help, and at the same time being constrained by Privacy
20 Act regulations and other sorts of things where you can
21 find yourself on the chopping block, so to speak, your
22 head, no matter what you do.

23 And to be quite truthful, I suspect in large
24 measure that our individual franchisees probably go out
25 on the line in terms of trying to help the Postal

1 Service and the FBI and the Secret Service, probably
2 beyond what they probably should in terms of the legal
3 perspective. And I shared that with Stacy and I say
4 that -- is somebody taking this down? I see somebody
5 over there is doing that. So, can we strike that last
6 part? [Laughter].

7 But I think that's a reality of the situation.
8 Our guys are local guys, they want to help, they want to
9 be -- they want to make -- do the right thing. I mean,
10 they're citizens, and they want to do the right thing.
11 And a lot of our guys are actually the people that tip
12 off the Postal Service as to things that are going on.
13 And we've received a lot of kudos in that respect.

14 MS. FEUER: Are there particular things -- when
15 you say that your CMRA MBE, in this case -- franchisees
16 are aware of that caused them to make that call? Are
17 there trends that you are seeing with respect to the
18 types of scams that you are seeing run through CMRAs?

19 MR. ARMSTRONG: Well, the scams have changed
20 over the years. When there's a crook, they're always
21 trying to think of a different way to use whatever they
22 can find to make a quick buck or two. But I think the
23 key thing that we have as an individual franchisee or
24 individual operator is what I call the smell test. I
25 mean, something just doesn't smell right. There's just

1 something that is not good about this. And our guys get
2 their antennas up.

3 Sometimes in that particular case, they'll take
4 the initiative and either call, not always is it the
5 Postal Service, it can be the local police, state and
6 local authorities. We get involved in a lot of the drug
7 scams. People use us as drops for drugs. That happens.
8 And that's outside of the Postal perspective, but that's
9 part of the world.

10 So, the key thing is to just be aware of what's
11 going on. And we do some things at MBA both at the
12 corporate level when we're training our franchisees and
13 at the local level with ongoing work with the Postal
14 Service. As a local franchisee in Maryland and DC, I
15 meet my franchisees periodically, and I can tell you
16 over the 15 years or so that I've been the area
17 franchisee, we've had the Postal Service in, for
18 example, half a dozen times over that period of time to
19 talk with us about how they operate and how we can be
20 helpful to them, and that sort of thing.

21 Now, this is all a very unofficial sort of
22 thing. There's nothing that requires us to do that.
23 We've just always done it because we thought it made
24 sense to do it. We want to be a good citizen. And we
25 are good citizens. We've got some good reps. At the

1 corporate level, we do so, as a part of training new
2 franchisees, but when we train new franchisees, we do
3 spend some time during our block doing lots of things,
4 and the CMRA part of it is just one part of it. But we
5 spend some time talking about fraud and scandal and how
6 we can be used and how the franchisee should be aware of
7 what's going on, both legally and also in terms of just
8 trying to do the right thing.

9 MS. FEUER: Thanks, Alan. I'm going to have
10 some more specific questions, but let me turn now to
11 Andy Lynn, and since Robin opened up the issue of
12 opening up courier packages that contain money, I'm
13 wondering what you are seeing at FedEx in terms of
14 frauds, particularly consumer frauds and what you do in
15 the first instance to address that.

16 MR. LYNN: Stacy, thanks a lot for inviting
17 FedEx to be part of your group here today, and I was
18 just looking at the list of folks here on this panel,
19 and the truth is, you know, FedEx works closely with
20 really all of these organizations on a daily basis. Not
21 quite as much of the Australian competition authorities
22 yet, but we'll be talking to you soon there.

23 But Robin and I were actually having a short
24 conversation before the panel, and I will tell you that
25 between the Customs Service and the Postal Inspector,

1 since we're carrying a lot of mail on our air network,
2 they can give you a very accurate idea of the sorts of
3 things that are moving through our system. You know,
4 there are all sorts of wrong types of shipments that can
5 move through the system, be it cash or contraband,
6 things of that nature.

7 I think Robin would tell you that the policy of
8 FedEx really from the beginning has been, number one, we
9 want to have, you know, a very close, cooperative
10 working relationship with law enforcement authorities.
11 We have a fairly large security organization, and a very
12 important part of their job is to liaise with the Postal
13 inspectors and the Customs and the FBI, and all these
14 other agencies that Alan was mentioning.

15 Do we have -- you know, again, between the smell
16 test, just in the express business, we have about three
17 million packages a day. It's hard to apply the smell
18 test to every single one of those, but the truth is
19 there is usually a FedEx courier or employee having some
20 interaction with the package. You know, are there
21 profiles and things that we look for that help us kind
22 of have a suspicion about whether something looks right
23 or not? Yes. Does the fact that we have a very
24 data-intensive, on the international express part of the
25 business, we gather a lot of information that's required

1 for our purposes for tracking, billing, and also for
2 Customs clearance.

3 So, we have a data-rich environment that, again,
4 we are able to work with law enforcement to use when
5 they say that they've got reasonable suspicion.

6 One of the things, Stacy, you and I talked about
7 leading up to this panel is that line that we really try
8 not to cross, which is we are about providing service to
9 our customers, we're about protecting the brand name,
10 the customer experience with FedEx. And let me just
11 disclaim any interest in our having or obtaining revenue
12 with working with fraudulent shippers. Let me tell you,
13 that's a bad business model for you. We have
14 salespeople that are focused on automotive industry,
15 health care, pharmaceuticals, we don't have a fraud
16 sales unit. We're not after those shipments.

17 Number one, they're not always the best to pay,
18 but number two, even if they do, at the end of that
19 transaction, you know, the bad guys are gone, the only
20 number they know is 1-800-GOFedEx and that can really
21 eat into your margins there.

22 But I'm sorry, my point was we want to work as
23 closely as we can with law enforcement and we do and we
24 will, but we mustn't let the FedExes of the world cross
25 over that line into actually becoming de facto law

1 enforcement agencies on their own. We have obviously
2 obligations to protect the integrity and the privacy of
3 data and people shipping legitimate shipments from point
4 to point need to not have an unrealistic fear that all
5 people who don't need to know their business are going
6 to know it.

7 MS. FEUER: Thanks. Before we turn to talk
8 about maybe some of the specifics of cooperation short
9 of co-oping private business into our line of work, I
10 just want to ask Lee about her experience in Australia,
11 and I know it's slightly different there because your
12 relationship with the Postal authorities is different,
13 but what do you see as the use of courier services and
14 CMRAs to the extent they exist in Australia?

15 MS. HOLLIS: Thank you, Stacy. I would just
16 like to say, by way of introduction, that as far as
17 cross-border fraud is concerned, apart from the net,
18 mail-based fraud is the next biggest issue for us. What
19 we have found in practice is that there is a great deal
20 of cooperation from commercial enterprise as well as our
21 Australian Postal sources in helping to detect and put
22 an end to cross-border fraud, particularly international
23 fraud.

24 There are legal impediments which affect how we
25 go about doing things, but I think generally, as has

1 been mentioned by members of the panel, we proceed from
2 the basis that no reputable company would want to be
3 associated with fraudulent conduct, and from that basis,
4 it's very easy for us to go ahead with commercial
5 enterprise to put a stop to fraud where that is
6 possible.

7 We do have issues in the international arena
8 with extended reshipping of checks and cash which means
9 that's quite a long investigative trail from time to
10 time going around the globe. I think we've had traders
11 who might ostensibly be located on the Gold Coast in
12 Queensland, for example, in Australia, which is a huge
13 post office box center, and associated probably with
14 criminal activity, but in fact, the originator of the
15 scam may be in Canada or the U.S. The mail may be
16 picked up from post office boxes in Australia by someone
17 who is unfamiliar with the scam, they're merely paid to
18 pick up and reship material, and on its way to the
19 States or Canada it may go through ports such as Fiji
20 and other places.

21 But our experience, as far as working in
22 partnership with commercial enterprise is concerned, has
23 been positive. I think particularly directed towards
24 disruption, where we've become aware of frauds, we take
25 it up with the commercial enterprises and generally

1 receive cooperation. And I think our next step is to
2 work in greater partnership with commercial enterprises
3 as well as our Australian Postal authorities to take
4 more preventative measures to prevent cross-border
5 fraud.

6 MS. FEUER: Thanks, Lee. Alan, maybe my next
7 question will get to this, and if not, you can chime in.
8 I wanted to just ask, you know, obviously there's a
9 level of cooperation that's already ongoing, both with
10 the criminal agencies and civil agencies like the FTC,
11 but I wanted to ask if some of this could be done on a
12 more systemic basis, and I guess there are three areas,
13 and I've talked a little bit with Alan and Andy about
14 them.

15 One is in the information sharing area.
16 Is there some more systemic way that we can get together
17 to share information, and the one issue I want to raise
18 is an idea that Robin and I were kicking around, and
19 that's of given an organization like FedEx, a
20 corporation that uses a lot of automated systems, if we,
21 law enforcement, were to come to you with a list of bad
22 addresses, for example, Montreal, is there some way of
23 flagging that in your computer so that your agents are
24 aware that there might be something fishy about 400
25 packages going to a certain address?

1 Let me throw out two other things and then maybe
2 we can comment on them all. Another thing that
3 Alan was talking about was he was talking about MBE
4 University where MBE trains its 3,000 franchisees in the
5 U.S., as well as its global franchisees, and I guess the
6 question there is are there more opportunities for
7 training, and I know FedEx does a lot of training.

8 And then the third thing that I want to throw
9 out here, for enhanced cooperation, and ask for your
10 thoughts on all three, again, goes to suspension of
11 services. What do you do when you are aware that
12 consumer frauds and money are being run through your
13 companies, and in terms of working with a civil
14 enforcement agency like the FTC, what do you need from
15 us to suspend those services? Do you need a court
16 order, or is there something less, given by the time we
17 go get a court order, sometimes the fraudsters will have
18 moved on.

19 So, I throw out all those questions and perhaps
20 Andy and Alan can take a stab at them.

21 MR. ARMSTRONG: All three?

22 MS. FEUER: Well, in the interest of time, I
23 figured I would lay it all on the table and then see
24 what people want to say.

25 MR. ARMSTRONG: Okay. Just two things, before

1 moving on to those things. First of all, although this
2 is called a commercial mail receiving CMRA panel, so to
3 speak, the fact of the matter is that not all the things
4 come through the mail in terms of fraud. I mean, we
5 take packages in as commercial mail receiving folks from
6 not only the mail, but also from FedEx and UPS and DHL
7 and Airborne and what have you, and it's just as likely
8 that those guys can be used for fraud and that sort of
9 thing as the Postal Service. I mean, it happens.

10 In fact, some of the biggest frauds that we've
11 been involved in very truthfully have come where we've
12 gotten involved in FedEx and UPS, because we accept
13 packages, and that's not really controlled by the CMRA
14 regulations. I mean, when we take a package in from
15 FedEx and UPS, not part of the CMRA regulations at all,
16 it's just receiving a package from FedEx.

17 The second thing before we move on, what is the
18 cost of the individual operator, the individual CMRA in
19 terms of this whole thing of fraud situation. Well, the
20 biggest cost for us is our credibility. My worst
21 nightmare as an area franchisee is to come home and be
22 watching the 6:30 news and all of the sudden find one of
23 my centers in downtown Washington, DC on the 6:30 news
24 talking about it's a drop for some criminal or
25 fraudulent scheme. That doesn't do us any good. And

1 that is just disastrous to us.

2 And it happens. And it happens across the
3 United States. So, we're very concerned about this from
4 a credibility perspective. That's critical to us,
5 because it strikes to the heart of our brand and our
6 operation. I wanted to get those two things out and I
7 think it's critical, you know, very important, those two
8 things.

9 Now, moving on to how we work with these folks,
10 most of our relationships right now have been pretty
11 informal. I can say this, and my colleague here from
12 the Postal Service might not even be aware of it, but we
13 have developed a pretty good relationship with one of
14 his colleagues out on the west coast at the national
15 level, and he funnels our folks at our corporate level
16 all kinds of information about what's going on in the
17 Postal Service, both through the scams and abuse that we
18 then download to our franchisees through internal
19 communications tools. And that's a very good way to do
20 it.

21 I mean, we did something about once a week from
22 our corporate headquarters talking about what's going
23 on, newsy sorts of things in our business. And it's
24 probably at least every -- out of every two or three of
25 those, there's something we receive in the Postal

1 Service saying watch out for this, watch out for this
2 name, watch out for this scheme that's going on. And I
3 think that's done unofficially, Larry, I don't think
4 there's anything official related to that. But it's an
5 excellent tool, by the way.

6 MS. FEUER: So, using your internal corporate
7 communications and having the Post Office provide that
8 information?

9 MR. MAXWELL: Yeah, what you said is totally
10 accurate. When we did the regulatory changes, one of
11 the understandings we had with the different
12 organizations, Charmaine as well, it would be nice if
13 she could address this with us, we agreed that we would
14 enhance our communications in terms of training and
15 sharing of information. We shared email addresses from
16 inspectors, that was done on a national level. I think
17 it's been better served at the local level up until this
18 time.

19 There's another group that's in charge of
20 identity theft in my organization that has
21 responsibility for that, and they're working now towards
22 organizing something a little bit more formal from the
23 national level. I think there's a lot of opportunity
24 there, but I'm glad to hear that they kept it rolling
25 from the time we had the original discussions, because

1 that was good.

2 MR. ARMSTRONG: I mean, I think the whole
3 relationship has been pretty informal, very quasi
4 official, so to speak. And I think it's funny in
5 talking about that, to make it more formal would be
6 very, very useful. Particularly at the top levels. I
7 mean, at the lower levels this sort of back and forth is
8 going to happen. Talking about not only from the Postal
9 Service, but the FTC and the Secret Service and anybody
10 else. We have a tremendous internal capability to get
11 the word out to our guys, and I don't think it's being
12 fully utilized by the rest of you all.

13 MS. FEUER: And we at the FTC would be very
14 happy about that. I mean, one of the things we talked
15 about a lot yesterday in our panel, since we obviously
16 have a lot of representatives of other law enforcement
17 agencies here, is how we can make sure that our efforts
18 are coordinated and that, you know, Larry, we work with
19 a lot, so he is aware of the scams that we're
20 investigating, but I think there is an opportunity, it
21 seems like, both with a corporation like MBE and FedEx,
22 to partner using the corporate communications systems
23 and that we in the government need to be feeding the
24 data and the trends we're seeing in a perhaps more
25 unified way.

1 MR. LYNN: Stacy, I think there are probably
2 opportunities to leverage communications networks that
3 we have. FedEx, you know, we've got an internal
4 television network and we do ongoing training and
5 safety, security, fraud detection, it gets right in
6 there along with how to be safe in bad weather and not
7 having vehicle accidents, but we would be very happy to
8 talk to you about featuring you folks on some of our
9 shows to say, here are some of the examples of things to
10 be looking for, and more importantly, here's what to do.

11 What we would probably do is feature the law
12 enforcement representative along with one of our
13 security folks, which gets back to your point on the
14 hypothetical about comparing a list of addresses and
15 seeing what can be done to sort of see what's happening
16 there. And what I would tell you is our informal
17 cooperative system would already facilitate that. I
18 would tell you to call me, call our security group, we
19 would sit down with the law enforcement officer and
20 evaluate the information and to the maximum extent
21 possible we're able to cooperate to get the bad guys.

22 As far as suspension of service, there are some
23 times when we need to suspend service to customers for
24 non-fraud-related matters. So, we have ways to do that.
25 Again, it would just involve our sitting down and

1 looking at what is the nature of the information and not
2 turning off any people that were actually not bad guys.
3 That's kind of a problem.

4 MS. FEUER: Right. And let me ask Larry or
5 Robin or both of you, in terms of some of these ideas of
6 continuing obviously the informal cooperation but doing
7 some more systemic things, you know, either on the
8 training end or the information sharing end, what do you
9 see as things that would be useful for you?

10 MR. MAXWELL: Well, I think we heard from John
11 Sullivan yesterday with the mail industry, and we've
12 done a lot of things there where we have joint meetings
13 and we share best practices. We have inspectors, some
14 of my counterparts work with FedEx, and they've come
15 back with glowing reports of your security network and
16 we've learned a lot from them and we've shared
17 information.

18 I think we can do a lot more from a systemic end
19 with the commercial mail-receiving agencies, which
20 frankly we probably let the ball drop. We could have
21 pursued it at an even greater rate to keep that rolling,
22 but I think our main focus was getting on the
23 registration and identification first and also the
24 database, but I think this next phase, there was talk of
25 having agents at training academies for new franchise

1 operators. Again, we've talked about uses of the
2 satellite networks, and I know there are some other
3 forms we could probably use for that.

4 The prevention area, of course, is always the
5 one we wanted to push and we try to share that. Any
6 time we do stand-up talks to Postal Service, to the
7 carriers, any time you have a false address, or in the
8 commercial agencies, you have issues which bring it up
9 to the supervisor and they'll talk to the operator of
10 the commercial mail receiving agency.

11 So, there are a lot of opportunities there, I
12 think we've kind of just scratched the surface a little
13 bit, and that's why this is a good dialogue, because
14 there's a lot more things we can do.

15 MR. LANDIS: I totally agree, because most of
16 the dealings are with the security office, the banks or
17 FedEx or the money transmitters, and we like to get the
18 message out to the actual worker bees at the street
19 level out there looking. They have more eyes out there
20 that can tell us a lot more of what's going on.

21 And I'll just give you a real fast story that we
22 discovered up in Montreal is that these people are very
23 well organized. They'll do surveillances at locations
24 for drop sites. They'll pick Stacy, they'll look at
25 your house, they'll see when you're home and when you're

1 not home. If you're not there between the hours of 8:00
2 and 5:00 and there's nobody else there, they will use
3 your name and your address and receive, and they will
4 have somebody sitting out in your driveway until that
5 package shows up. And they say, oh, I'm Stacy, I'm just
6 getting ready to go to work, I'll take the package. And
7 then when law enforcement comes knocking at the door,
8 they're looking for Stacy for receiving the money.

9 I mean, these guys are very well organized. And
10 when you have more eyes out there like the drivers,
11 saying, hey, this doesn't look right. Or if we have the
12 drop sites, where mail is being forwarded in large
13 quantities for a foreign country, if they have a box
14 with a return address that's different than where
15 they're located, and sweeps. Sweepstakes, entries, and
16 this I would like to stress this to everybody, any time
17 a sweepstakes asks for your private home phone number,
18 you're asking for trouble. That's what we find at 90
19 percent of the telemarketers, the fraudulent
20 telemarketers are people that put their phone numbers on
21 sweepstakes. And that's what we're finding.

22 MS. FEUER: Let me just ask Lee, before we move
23 to some questions from the audience, you said that you
24 had generally very good levels of cooperation, and I'm
25 wondering if there was a particular example of something

1 systemic you do or something informal that has been done
2 that might serve as a model for us here?

3 MS. HOLLIS: Well, I would refer to the general
4 situation where we have good liaison and relations with
5 The Directing Marketing Association in Australia, and
6 the members include frank companies, and through that
7 forum, it's a very good way to liaise on a regular
8 basis, and find out how industry is viewing the world
9 and what's going on. And particular areas or hot areas
10 that might be developing and emerging, and also a chance
11 for us to give something back to industry through that
12 forum.

13 MS. FEUER: And that's great and that will
14 actually lead us into our next panel this morning. I want
15 to just leave it open for any final
16 comments from the panelists, and also turn to the
17 audience and if anybody has a question to raise their
18 hand and we'll bring the wireless mic over.

19 Elliot, if you could identify yourself for the
20 record.

21 MR. BURG: Elliot Burg from the Vermont Attorney
22 General's Office. I had a question for Andy. I take it
23 from what Robin has had to say is that there's still a
24 problem with courier services picking up checks from
25 consumers' homes. If that's the way physical checks are

1 making their way to Canada.

2 If that's true, or to the extent that it's true,
3 does FedEx have procedures in place for its delivery
4 people, procedures and training that would allow those
5 people to sort of -- I want to use this in a benign way,
6 but profile the people that they're picking up mail from
7 to determine if they've got a potential victim. Maybe
8 it's not an elderly person, but some situation where
9 they can spot a victim of fraud and then try to educate
10 the person or persuade them not to go forward with the
11 delivery?

12 MR. LYNN: I think, again, you've touched on a
13 very good example of that balancing act that we have to
14 perform every day. I mean, the truth is, our couriers
15 tend to know the people, and we're really talking here a
16 residential situation, and probably the most effective
17 deterrent that we have is just sort of the gut feel of
18 our people. And there are certainly anecdotes where
19 I've been involved where we get this call and someone
20 just says, you know, this just doesn't feel right.

21 So, we've got 45, 50,000 couriers on the
22 streets, and they're mainly nice people and they mainly
23 like their customers, but if you take your question kind
24 of just a half step further, there's really not going to
25 be a way for FedEx or any other entity to sort of be the

1 guarantor of the integrity of the transaction that
2 they're a part of.

3 You know, just as the mail, you know, the Postal
4 Service, we do what we can to keep the bad guys at bay,
5 we really want to do that, but we're not going to be
6 able to get to the point, I don't think, of asking 20
7 questions about all right, Mrs. Johnson, why exactly are
8 you sending this check to ABC company, have you thought
9 it through. There's a point at which nobody can
10 completely protect people from fraud, but we certainly
11 are interested in doing it, and our people, our couriers
12 especially, use their judgment very well in that regard.

13 MS. FEUER: And if I'm correct, you did tell me,
14 though, that from time to time FedEx will open packages
15 under your conditions of carriage.

16 MR. LYNN: We certainly have the ability to do
17 that. You know, the conditions of carriage, and it has
18 always been that way, but if in the example we're
19 discussing, we would open a package to see who the check
20 was made out to, I mean that doesn't exactly fit the
21 normal profile, but again, Robin and his band of
22 characters, of course, can open any international-bound
23 package that they want to.

24 MS. FEUER: And they do.

25 MR. LYNN: And they certainly do, and they have

1 data systems to, again, officially profile the packages,
2 and we do a lot of package opening.

3 MS. GRANT: Hi, Susan Grant from the National
4 Consumers League. Two things, one for Andy and one for
5 Larry. As an example of a proactive measure, Western
6 Union, when you call its quick pay service, actually has
7 a recording that says that if you're trying to send
8 money for a sweepstakes or to make a charitable donation
9 to firefighter or law enforcement organization, press 1,
10 and then when you do that, you get a message saying
11 essentially that it's a scam.

12 That's a good model that could be used whenever
13 consumers are making arrangements by phone, and also if
14 somebody is going to a house to pick up a check, perhaps
15 there could be some written information that is given to
16 them about scams and how they work and how to recognize
17 the danger signs that might forewarn the consumer that
18 maybe they're about to do something about.

19 So, that would be interesting to consider.

20 An issue for Larry, as you know, we were really
21 unhappy with the alternative in the CMRA rules for the
22 hatchmark number in the address, because there's no way
23 that consumers can tell from that that they're not
24 sending a payment to a suite in an office building,
25 whereas PMB is much more obvious. It would have been

1 much easier to train consumers that when you see PMB,
2 what that means.

3 We're not finding that anybody is using PMB.
4 So, I've got a couple of questions for you. One is, are
5 you finding that anybody is using PMB, and are you
6 finding that the cross or pound sign number is being
7 abused? And also, will the Post Office deliver the mail
8 to the commercial mail receiving agency if it doesn't
9 have either PMB or the hatchmark?

10 MS. FEUER: Why don't we have Larry answer and
11 then I don't know if Andy wants to comment on Susan's
12 question.

13 MR. LYNN: Go ahead.

14 MR. MAXWELL: Susan, with the pound sign, I
15 haven't seen any -- I've seen both used, I've seen PMB
16 and pound sign used. Pound sign is a little harder to
17 distinguish, because it can get merged in with some of
18 the other address aspects, and that is one of the things
19 that did concern us. But the PMB I have seen used, and
20 if they're not using either, the Post Office is under
21 the directions to discuss the matter with the CMRA
22 operator.

23 Stacy raised the issue of what alternative means
24 we have as far as shutting down and so forth. That's an
25 extreme measure. The Postal Service has that ability,

1 the district manager can shut down a CMRA franchise if
2 they're not in compliance, if they're found not to be in
3 compliance. And naturally nobody wants to do that, and
4 so far we haven't had to do that. And they've been in
5 compliance. And if there is a customer, one customer,
6 that's out of compliance, they're not going to risk
7 having -- and that's the whole theory behind that.

8 What I am doing as we speak, in fact, we're
9 looking at a means to take the 1583-As, which is the
10 CMRA operator, their application, that's not automated
11 nationally. We would like to automate that nationally
12 for our purposes just to help address the issue of this
13 is a CMRA, this is a listing, and at least make that
14 available so if you're mailing to it. Because right now
15 it doesn't exist with us. It exists with the industry,
16 separately. It's not all pulled together. And I think
17 that most people have been asking for that and it's just
18 never -- there was never a need before and you can
19 imagine, with 40,000 post offices, and a lot of them
20 aren't regulated. A lot of them don't even register
21 that are in the legitimate side of the industry.

22 If you go into the Bronx or Queens or even areas
23 of DC, you're going to find a lot of what we call
24 mom-and-pop stores where they will take mail in for
25 people. And, again, that's a postal delivery issue, we

1 shouldn't be delivering mail if we don't know who that
2 is, but it does happen.

3 MR. ARMSTRONG: Stacy, can I kind of follow up
4 on that? As it relates to the PMB, it is being used.
5 What we do with new potential customers who rent
6 mailboxes is explain to them how they should have their
7 mail sent to us and what have you. But in a very
8 practical sense, we in the CMRA industry can do our job
9 by informing customers this is how you mail things or
10 have things mailed to you. But when they go out and
11 communicate and portray their address on the one hand,
12 and how the people who send things to them use their
13 address is impossible to regulate. I mean it's just
14 impossible.

15 You know, if somebody decides to send me a card
16 and how they put the address and how they lay it out,
17 regardless of what the regulations have, you know,
18 what's the practical answer to that? I don't know the
19 practical answer to it. It's very, very difficult,
20 though. But we can and we do do everything we can, and
21 you say there's been no CMRA so far that you're aware of
22 that you guys have had to put the hammer on?

23 MR. MAXWELL: No, there was one, there was a
24 little discussion over some issues with one customer,
25 but we talked about that and calmed that down.

1 MS. FEUER: Andy, did you have any response to
2 that?

3 MR. LYNN: On your issue, number one, it would
4 be very interesting to hear any specific anecdotes that
5 you've got about somebody having to go out and pick up a
6 check. I am going to tell you, I don't think we're too
7 out of school to say that in the type of scam that
8 you're describing where you have the boiler room
9 operator saying, all right, I'm going to have a courier
10 come out to your location and pick up a check, the good
11 news about those is that those are typically, they're
12 going to need to be billed to an account number, and it
13 is easy once we are able to identify these as bad
14 actors, you know, in our systems, you know, to kind of
15 make that stop.

16 You know, the bad guys are agile and move
17 around, but it would be a bit of an atypical situation
18 for someone who doesn't have an account number with us
19 already shipping FedEx Express, for example, to call out
20 and have a courier come to pick up a check.

21 I've taken a long time to say, we're always open
22 to other suggestions on how to improve our
23 communications and our screening, but what I would tell
24 you is that I think our current mechanisms are fairly
25 good in that regard and there usually has to be one or

1 two victims before we catch the bad guys, but we can get
2 them pretty quick.

3 MS. FEUER: Great. I think what we'll do now is
4 move on to the next panel, so I want to thank all the
5 panelists here for participating. It is a shame
6 that Charmaine Fennie wasn't able to join us, although
7 she got a lot of references, and we've heard a lot of
8 positive things about what's going on now and perhaps
9 ways to build on that with both the CMRA industry and
10 with courier services like FedEx. So, thanks a lot, and
11 we will move right along to the next panel on the role
12 of self-regulatory organizations and industry
13 associations.

14 (Applause.)

15 MR. STEVENSON: All right, well, why don't we
16 move on to our next panel, which is the role of industry
17 associations and self regulatory organizations and the
18 role that they might play. And we have -- I think the
19 panelists' bios are in the material, so I just propose
20 to jump right into the discussion, and I think that the
21 question to start with is what role is it realistic to
22 expect that industry associations might play in
23 partnering with law enforcement? Obviously there are
24 roles that they have, legitimate roles in advancing the
25 industry's other interests with law enforcement, but

1 what kinds of roles is it really realistic to expect
2 that industry associations can play in partnership, and
3 how might we see them, what kinds of examples do we
4 have?

5 And I'm going to actually look for a volunteer
6 to answer that question, if somebody wants to put a tent
7 up and venture a thought on how they might see that
8 question. We will have a volunteer, even if no one puts
9 their tent up, but --

10 MR. WHITELAW: All right, all right.

11 MR. STEVENSON: Bob Whitelaw?

12 MR. WHITELAW: Yes, I think number one in terms
13 of the Better Business Bureau system, there is no
14 border, no cross-border matter, and that with our
15 counsel in Arlington and the counsel in Canada, we share
16 a lot of information. And on the positive point, we're
17 not bounded by a lot of regulatory requirements.

18 The best way of the partnership and idea is Ken
19 Hunter, former Chief Postal Inspector of the United
20 States, has sort of put our mandate up, and that is when
21 a consumer, a business, or an organization is about to
22 spend money or donate money, we want to be there to
23 reduce their risk.

24 Now, we, in terms of receiving information, have
25 the opportunity to deal with awareness, accessibility to

1 just-in-time information, responsiveness, and
2 redirection, and without too many seconds passing, we
3 can get information out to the bureaus, the 140
4 throughout North America instantaneously. At the same
5 time, move information to the media, and more
6 importantly, to governments, whether it's the
7 Competition Bureau in Canada, the Federal Trade
8 Commission, the Office of Fair Trading, move that out,
9 get it out to the business community.

10 Almost in an, as I say, within seconds of
11 information, that's one of the main tools of this
12 regulatory or nonregulatory work that we do without
13 having the checks and balances. We can name names. We
14 can name issues. We can name addresses. And that is
15 helpful to consumers, businesses, organizations, and
16 government groups.

17 MR. STEVENSON: Let me ask, maybe Mark Bohannon,
18 we were talking earlier about this issue and the kind of
19 role that the industry associations might play, and it
20 may be also obviously that industry association may mean
21 something slightly different from the role that the BBB
22 can play, but, Mark, I think you had a few thoughts on
23 that.

24 MR. BOHANNON: Yeah, sure. I appreciate your
25 comment, Hugh. We are not a Better Business Bureau,

1 though we have tremendous respect for what the Better
2 Business Bureau does. We are an association that has
3 companies as members. Those companies range from some
4 of the smallest in the technology area to some of the
5 largest, and even, you know, along that range, they face
6 a variety of fraudulent acts, both here in the United
7 States and abroad.

8 So, that is an area particularly in what I would
9 call and what you probably understand as the
10 counterfeiting areas, a place where we do a great deal
11 of work with a variety of law enforcement authorities
12 here in the U.S., and as appropriate and others,
13 particularly Canada, Mexico, and to some degree the
14 United Kingdom.

15 We see and are asked by our members to play a
16 variety of roles in working with law enforcement. They
17 range from being a source of information and helping to
18 keep government enforcement authorities up to date on
19 new models of what we see as fraud and counterfeiting,
20 in a world that advances as technologically quickly as
21 our world does, it is a challenge for everyone to keep
22 up with what is going on in the new models and
23 approaches to fraud, and certainly we see our role as
24 being both a formal and informal source of helping to
25 understand what those new models are.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

1 And we do that through white papers, which you
2 will find on our website, we do it through informal
3 dialogue, we go to meetings, and quite frankly
4 responding to calls as appropriate.

5 The second role that we often and significantly
6 play is being an interface between our member companies
7 and law enforcement in situations where either there may
8 be criminal or civil action brought against someone, and
9 where the company either does not have the bandwidth or
10 is not comfortable with being a direct interface as
11 well. That often involves in our case being a hotline
12 for tips for those who pirate or counterfeit our company
13 products. We have a very sophisticated operation that
14 goes back at least 15 years working in this area. We
15 have clear issues and policies about the anonymity of
16 that data, and at the same time, over the years, we have
17 developed a solid reputation with law enforcement that
18 what information you get from us is going to be very
19 real and very serious.

20 And I think the third area, as appropriate, is
21 coordinating on appropriate enforcement actions when
22 fraud is actually found. The reality is that both in
23 the public and private sectors, there are not all the
24 resources to go around. In some cases, it is
25 appropriate to bring criminal action, some cases it's

1 not, and so as appropriate, and within appropriate
2 boundaries, those are areas where we interface as well.

3 So, Hugh, those are some of the examples. I
4 would be glad to explain more, if you want me to go into
5 more detail.

6 MR. STEVENSON: Thank you. Maybe I would ask
7 next Jerry Cerasale how the experience with the
8 Directing Marketing Association compares with the
9 experience that Mark just described for the Software
10 Information Industry Association.

11 MR. CERASALE: Thanks. The Directing Marketing
12 Association has its own internal guidelines for its
13 members and an ethics procedure dealing with and split
14 up in two with telemarketing and then all other ethics
15 procedures.

16 The goal of that kind of self-regulation is to
17 try and get things corrected, but if we find in the
18 course of this investigation, which is done by peers of
19 the member companies, and we have no individual members,
20 but 5,000 corporate members, we will then transmit the
21 information we find to the appropriate legal
22 authorities. If we find, in fact, there appears to be a
23 violation of law, be it the state AG, be it the Federal
24 Communications Commission, the Federal Trade Commission,
25 et cetera.

1 One of the things that where we really work well
2 with the Postal Inspection Service, and I think you had
3 a member of the panel yesterday discuss it, bad
4 addresses, identity theft kind of things where an
5 identity theft is a crime against me, the individual,
6 it's also a crime against me, the company, if you're
7 going to try and purchase something and end up not
8 paying for it.

9 So, there are a lot of addresses that where that
10 happens, and that information gets out and you know that
11 123 Main Street of this town is generally an address to
12 be leery of, and we work with that with the law
13 enforcement community and spread that word around,
14 because that can help prevent a continuation of the
15 fraud and try and find someone.

16 A lot of times the cross-border fraud,
17 unfortunately, except for the lottery issue that was
18 raised, I mean that's illegal on its face, and members
19 should know that, they're required to know what kind of
20 pieces go out and how lists and so forth are being used.
21 But many times, the fraudsters break up their
22 activities. They may control the telemarketer located
23 in Canada, we're dumping on our poor neighbor in the
24 north, but located in India, located in Bangladesh,
25 anyplace where they think that they can go into the U.S.

1 where there's a different English, or even a Spanish
2 country if they want to come into Spanish-speaking
3 Americans and so forth, they can control them.

4 But they get a list from somewhere and the list
5 provider takes a look at the script and the script looks
6 fine, because the fraud happens with, I send the money
7 in and I don't receive what I paid for. And they could
8 use a printer, the printer, the printing looks fine, it
9 could be a very legitimate offer, if, in fact, they do
10 that, and so you don't know.

11 And so that's part of the problem that we face
12 from the point of view of this type of fraud, which we
13 all want to try and get ahold of, even information, if
14 it's not obvious on the face of the piece of the
15 campaign that you're dealing with, you're not going to
16 catch it. It's a requirement of our members to take a
17 look at what your piece is, what the piece of this
18 campaign is. If you're sending a list, what's the
19 providing list being used for? Well, it's being used to
20 sell such and such. And you send the money in and you
21 don't get it back.

22 Well, the list owner is not the fulfillment
23 agency, so they're not aware of it. They can even see
24 the list, so that you're going to call Jerry Cerasale's
25 home, even though I'm not on the -- normally on a list,

1 I'm just going to see what's being said and I can listen
2 to the script, say, no, I'm not interested, because I'm
3 not going to spend \$1,000 or the \$100 or whatever it is,
4 but the script sounds legitimate. And that's part of
5 the problem that we face.

6 So, I think that if we find information we have
7 to get it to you. And we have to work, I think, within
8 our DMAs throughout the country. You heard about
9 Australia working with their authorities, and Alistair
10 is here, as direct marketing associations have to work
11 together to try to spread information. I think that's
12 the biggest key. The problem that we all face, though,
13 the one fear, and I'll just say it, is spreading the
14 information, does it make you automatically
15 knowledgeable and liable for it, and therefore our
16 members will then not become volunteer members of the
17 association any longer. So, we have to worry about that
18 kind of thing.

19 MR. STEVENSON: Okay. And that's an interesting
20 point. And maybe, as I understand it, just by way of
21 background, a lot of your members are indeed suppliers
22 or the service bureaus who are involved who might be the
23 entities who were seeing these various pieces that you
24 describe, and so one of the challenges is the role that
25 they're playing, and you're talking about their

1 incentives to be a member of your organization.

2 MR. CERASALE: Right. And, I mean, it is --
3 they don't want to -- as they said in an earlier panel,
4 you know, having a fraud model is not a good business
5 model generally for a legitimate business player, but
6 how do they know? Because in essence, there's the
7 fraudsters are putting a fraud upon the suppliers, some
8 of the suppliers, anyway, using their facilities to
9 perpetuate a fraud, but keeping that knowledge away from
10 the supplier. And we have a lot of suppliers.

11 MR. STEVENSON: And, Jerry, I know the DMA has,
12 I think you referred to this briefly, a code of conduct
13 that applies to the various members, and I think there
14 are provisions on the supplier service bureaus. Is one
15 possibility, of course, there is the fear that you
16 mentioned, but is one possibility thinking about
17 adjusting that code in some way so that people are --
18 have some role in trying to see the larger picture?

19 MR. CERASALE: I think that we -- I think that's
20 worth a good series of discussions as we come out of
21 this and what the authorities do, what the Federal Trade
22 Commission wants to do, and try and get our -- not just
23 us, but the international brotherhood, and Alistair may
24 talk to that, of the DMAs, to take a look at what type
25 of thing we can do and how we can make an adjustment. I

1 think that that makes some sense, because, you know,
2 fraud hurts the entire business, so it hurts our
3 legitimate members to have cross-border fraud. So, you
4 want to try and end that.

5 But working it that way, but not becoming the
6 police force on our own sense, because we can't, that's
7 not our role, and but to work in that way, I think, yes,
8 we can look at that, we can try and see what we can get
9 together, what law enforcement needs, what we're able to
10 provide and so forth.

11 MR. STEVENSON: Can you say just a little bit
12 more about the fear issue, or the liability issue, maybe
13 just to spell it out, put that on the table. What, sort
14 of, are the bad things that could happen there?

15 MR. CERASALE: Well, I think the bad thing that
16 can happen is that you suddenly don't have people being
17 members of the DMA if, in fact, we work with law
18 enforcement. And we get information that we distribute
19 to our members. And then that becomes, in legal terms,
20 actual knowledge, and therefore then the supplier would
21 then be held because the DMA put this information out,
22 to then become a knowing participant in the fraud.

23 That's the kind of thing that we have to be
24 careful of, not to cross that line, because then that
25 becomes a disincentive for even legitimate companies who

1 could be caught up with a small piece of someone
2 purchasing something from someone to drop out of the
3 membership and then that would lose, it would hurt DMA
4 and it would hurt me, since it would be my salary, in
5 part, but it would also hurt the cooperation side, if
6 you have outliers.

7 Now, some of the suppliers in these frauds are
8 clearly legitimate companies that are probably members
9 of many organizations and want to do well. Others
10 probably may not be, but at least you want to keep the
11 good guys that are there trying to work in that
12 direction and not give them a disincentive not to
13 cooperate, in that sense.

14 MR. STEVENSON: Okay. Maybe we'll turn now to
15 Alistair Tempest, and your role that Jerry described as
16 the international brotherhood, or at least the
17 international aspects of direct marketing associations,
18 and how do some of these concerns that Jerry mentioned
19 play out internationally? I guess one thing I'll
20 mention to put this in context, and Jerry referred to
21 this briefly, but this issue which is the outsourcing of
22 various capacities.

23 There was a cover story on a recent business
24 magazine about call centers being outsourced, and they
25 cited to the Philippines, to India, to Costa Rica, South

1 Africa, Mauritius. I mean, this is a phenomenon in
2 terms of how the legitimate industry is going, I take it
3 that's fair to say, and so that raises the question of
4 what implications does that have for the illegitimate
5 part of the industry, and is there a role that the
6 related organizations can play in addressing those
7 problems?

8 MR. TEMPEST: Thank you very much. Well,
9 firstly, I would just like to comment very quickly on a
10 point. You said the illegitimate part of the industry,
11 of course it's not part of the industry. We would get
12 rid of it if we could.

13 Turning to what brother Jerry said, from the
14 brotherhood, we're faced -- perhaps I should say a
15 little bit quickly about Europe, because it is somewhat
16 more complex. In Europe, we're faced with a patchwork
17 of regulations, self-regulation, which makes things very
18 difficult. In some countries, self-regulation is very
19 well developed, particularly, for example, in the
20 country that I originally came from, the UK. In some
21 countries, for example Germany, the law is used.

22 There were some lovely statistics some years ago
23 where the advertising standards authority of the UK were
24 looking at something like 2,000 cases, and about
25 something like 60 were going to the courts eventually.

1 Whereas in Germany, exactly the opposite, there were
2 about 2,000 court cases, and only about 60 cases going
3 to the self-regulatory body and there was that overlap.
4 So, you can see from that that there is a very big
5 difficuly in giving an easy answer to your questions in
6 Europe.

7 What we clearly want, and I want to stress very
8 much what Jerry said, the issue of confidence in direct
9 marketing is very much at stake here. If there is more
10 fraud, then the more fraud there is. And I would
11 include within fraud harmful spamming. Then direct
12 marketing and the acceptance of direct marketing starts
13 to be very, very seriously undermined. I think that we
14 can see some rather nasty experiences in Central and
15 Eastern Europe where the people were much more naive
16 because they had never been approached before, and then
17 of course you've got the fraudsters going in doing all
18 sorts of perpetrating or all sorts of crimes against
19 humanity, imparting from the unfortunate consumers large
20 amounts of money, at least relatively large amounts of
21 money.

22 Now, in some countries, for example in Poland
23 and the Czech Republic, there is a resistance building
24 up to buying at a distance, within their own country,
25 farther outside. So, one has this serious problem

1 starting in some of the new democracies. As I think
2 Donald Rumsfeld recently called it, the new Europe, the
3 new energetic Europe, not the old tired Europe.

4 So, in terms of looking at the way in which
5 self-regulation is operated in Europe, we at FEDMA have
6 a number of codes, we have a code on e-commerce, we have
7 a code which is being negotiated with the regulators on
8 data protection or data privacy. We have codes on list
9 brokers, we have codes on telecommunications --
10 teleservices, and we support the preference services or
11 Robinson lists at the national level.

12 We can only do that through the national level,
13 and with the support, of course, of the national level,
14 and of the direct marketing associations at the national
15 level. Or if it isn't a direct marketing association,
16 sometimes it's a self-regulatory body. What we're also
17 doing, as Charlie Underhill mentioned yesterday, is
18 working with the Global Trust Alliance, very much, to
19 try and build that up on the global level.

20 What we, I think, what I would like to say is
21 that I feel that there is a problem, a problem not only
22 in Europe, but also outside Europe as well, where
23 different authorities and different organizations and
24 different self-regulatory bodies are looking at
25 different means of communication, and that creates

1 artificial, particularly nowadays, artificial
2 differences in the way in which certain forms of
3 communication are dealt with. And that is a problem.
4 It creates a problem, because, for example, in
5 e-commerce, you may have one type of rules, created by
6 one authority, or one self-regulatory body, and in mail
7 we have something else. So, we have this unbalance.

8 MR. STEVENSON: Since you're tired, I don't want
9 to overtax you, but just to follow up with one question.
10 Jerry mentioned the DMA codes which do have some
11 provisions on suppliers and service bureaus, in other
12 words I'm thinking of the ones that apply to just the
13 third parties if you will, as opposed to the marketers
14 themselves. Do you all or do your members have
15 provisions like that? Is there a common thread in terms
16 of what those provisions provide for? Could there be?
17 Would there be some value in doing that, and would your
18 membership have the same fear that Jerry mentioned?

19 MR. TEMPEST: Hugh, thank you very much, indeed,
20 because this is a particular issue at the moment.
21 Firstly, again, I have to stress the difference from
22 country to country; however, having said that, some of
23 our members, for example, the one in Belgium, not only
24 has the right to fine its members, and indeed it's done
25 that if it can get at them, for providing services to

1 known fraudsters, but also there is a case which just
2 came up this week in the UK, the vice chairman or one of
3 the vice chairmen of The Directing Marketing Association
4 UK has been nabbed, I don't know if that's the right
5 wording in American, but caught because consistently her
6 agency has been providing services to a couple of known
7 fraudsters.

8 Particularly time share, time share is a big
9 thing in Europe, I don't know if it's so much here, but
10 this is one of the fashions now, so-called Spanish --
11 the Spanish fraud. And she has been -- she's been put
12 under investigation and is very likely not only to be
13 thrown out of her vice chairmanship, but even to have
14 her agency banned from the DMA UK. So, I think a very
15 good example.

16 Now, liability, we're not quite so litigious in
17 some respects in Europe. So, we don't have quite that
18 problem, except that I personally have that problem
19 being in Belgium, we send out alerts for our members
20 when we have well-known fraudsters wandering around.
21 Officially, I could be caught under Belgian law and
22 sued, because under Belgian law, I am not allowed to say
23 that. Under UK law, I could say that. So, it's a
24 problem.

25 MR. STEVENSON: Well, I would like to turn now

1 to our two law enforcements on the panel to get their
2 reactions to some of the comments, and I guess
3 particularly maybe the issue that the tension have
4 raised on possible liability and what effect that might
5 have, and maybe start with you, John Mercer, from the
6 Competition Bureau in Canada.

7 MR. MERCER: Thanks, Hugh, and I certainly
8 welcome the opportunity to be here in the last two days.
9 I found this an excellent dialogue.

10 On liability, of course, there is a potential
11 antitrust liability in terms of cooperation, and that's
12 a cautionary note, but it's the issue whereby within
13 trade associations, within self-regulatory groups,
14 people cross the line and go from that which relates to,
15 for example, fraud, and start dealing with competitive
16 variables that are important to a viable competitive
17 market, so it's just getting into discussions of price,
18 market sharing and so forth, and of course I know that
19 no one in this room would be tempted to do that. That
20 crosses the line, and that would cause concern, and that
21 certainly creates a liability.

22 I guess picking up on some of the other issues
23 that have been raised, I think it's very important to
24 know who your members are. I think that's another kind
25 of issue that has arisen, certainly within the Canadian

1 context, and some cross-border contexts. We have
2 certainly been dealing with some respectable --
3 apparently respectable marketers.

4 I remember a couple of years ago I went to a
5 concert and I opened the program and much to my shock,
6 the sponsors of the concert turned out to be somebody
7 who we were investigating and who was, in fact,
8 subsequently, he and his colleagues, were arrested, and
9 I guess faced some considerable time, and I guess time,
10 first, before the courts. So, that kind of thing
11 becomes very important as well.

12 Another thing is, know who you are supplying, if
13 you're a trade association, if your members are a trade
14 association. This is a good area in which there needs
15 to be dialogue. In Canada, we have under our
16 telemarketing law an injunctive proceeding against third
17 party suppliers, such as telephone companies and so
18 forth, who are supplying product to people who have been
19 across the line once in deceptive telemarketing.

20 So, that becomes an important element on the
21 liability side.

22 I guess the overall view, however, on the role
23 of the private sector is, first of all, we can't do it
24 alone. Law enforcement can't do it alone. We require
25 cooperation, we need cooperation, we need that informal

1 network. But the other thing is, public education is an
2 important vehicle here, because we're never going to get
3 all these people, and I would hope that the private
4 sector would get involved in such organizations as
5 NWCCC, National White Collar Crimes Center, and the
6 National White Collar Crimes Center Canada, which has
7 been set up in order to have that dialogue. It's a good
8 place for dialogue on trends in law enforcement, but
9 it's also a good place for assistance and perhaps
10 funding public education.

11 We have in Canada something called The Mass
12 Marketing Fraud Forum, in which we have involved a
13 dialogue with our partners in the United States, the
14 Federal Trade Commission, the U.S. Postal and the U.S.
15 Department of Justice, and what we need there, we have a
16 steering group which has private sector members, but we
17 also have a primary group that has private sector
18 members, and ultimately we will be looking to them as
19 well for funding out of their in kind, or through
20 dissemination. That also becomes important.

21 It's a way to protect both your members against
22 fraud and also to assist in sensitizing the public to
23 these kinds of fraud arches that are around. So, that
24 would be certainly a strong recommendation. And I guess
25 finally, one could talk about the codes of behavior and

1 enforcing those within the context of self-regulatory
2 groups or within certain trade association arrangements.

3 Thanks.

4 MR. STEVENSON: Thanks, Don. And you were
5 mentioning in making the defendants face the music,
6 reminds me I should mention to people that there is
7 going to be a press conference today, in case you're not
8 aware, here at I think it's 1:00, is that right, on a
9 joint Canada/U.S./Mexican enforcement initiative. So,
10 very timely, given the subject of our workshop.

11 Let me turn now to Dan Nathan who is with the
12 Commodity Futures Trading Commission in the United
13 States, but who is in a more specialized area but has
14 had some experience with dealing with the
15 self-regulation in that area, and Dan, maybe you can
16 react to some of the comments and particularly some of
17 the concerns that are raised here and how they play out
18 in your area.

19 MR. NATHAN: Yeah, thanks. Actually the
20 comments here are helping me focus my remarks. I came
21 to the FTC with the idea of speaking about the National
22 Futures Association, which is the self-regulatory
23 organization that assists us in regulating the futures
24 and commodities industry. I'm with the Division of
25 Enforcement, and as was just said, the government has

1 limited resources and we rely heavily on the NFA and
2 other SROs to help us do the work that we have to do.

3 When you talk about the liability issue, our
4 SROs may have an advantage over others, in that they are
5 protected and created under color of law. The NFA is a
6 registered futures association established under our act
7 and it is given certain powers and it has the ability to
8 take on more powers as they are delegated to them. Over
9 the years, the commission has made a habit, every so
10 often, of delegating more and more powers to the NFA to
11 help us in what we do.

12 The implication of your question, Hugh, as to
13 what role is it reasonable to expect a professional
14 organization to play, I guess is that there are
15 limitations, possible limits on the aggressiveness or
16 effectiveness of professional organizations as to who
17 they represent, who pays their freight. They're
18 professional organizations and they have members, in
19 addition to maybe limits on their authority, and there
20 are also liability issues. Based on what I'm hearing
21 here, and based on what I have seen in my own
22 experience, I don't see a problem with the first prong.

23 The NFA specifically views it in their interest
24 as being in their interest to make sure that the futures
25 industry has kept clean, that those members who are

1 above board and are not, you know, scamsters, are
2 thriving in an industry that is not dragged down by the
3 bottom dwellers. So, they're doing everything they can
4 to keep things clean there.

5 On top of that, what I think I've noticed, and
6 they do an excellent job, and although I'm not typically
7 a believer in government competing with the private
8 sector in certain roles, for example school vouchers, in
9 this case, I see it as functioning very well. We have a
10 very aggressive enforcement division, and they have a
11 surveillance and enforcement group, which is similarly
12 very aggressive and we are always trying new things.

13 We both have a fair amount of flexibility,
14 although I have to say, being nongovernmental, being
15 essentially a private sector organization, the NFA has a
16 great deal of flexibility in the ways that it can
17 investigate and the types of evidence that they can
18 gather and the uses to which they can put it. And
19 there's a sort of spur to friendly competition. We egg
20 each other on. And at the same time, we work and
21 coordinate very closely together.

22 The second area in which the NFA and other
23 professional organizations or SROs might be limited is
24 simply limits on their authority. We as a governmental
25 entity have the ability to subpoena, we have extensive

1 information-sharing agreements with other nations, and
2 we can obtain a lot of information that they cannot
3 obtain. And that is where we come in. We carry a
4 badge. We have the ability to gather that information,
5 so when the NFA and we coordinate on what we're doing,
6 which we frequently do, we speak every month, we meet up
7 at a number of association meetings, we talk about what
8 we're doing and we divy up our work.

9 All of the day-to-day, mainstream kind of
10 bread-and-butter customer fraud type cases, single
11 brokers ripping off single customers, the NFA generally
12 handles. They have a full docket of those cases,
13 they've become quite expert at doing them, and they
14 generally end up in finance that are sufficient to --
15 and penalties sufficient to put people out of the
16 industry for some time and hopefully reform them or keep
17 them out forever.

18 The larger matters, the more systemic matters,
19 the matters that cut across both the regulated and
20 unregulated industry are the ones that we take, and we
21 take them usually with some help from the NFA, in the
22 audit functions that they execute, in the document
23 review functions that they carry out, and we take those
24 and then finally we come to one reason why we're here
25 today, cross-border.

1 NFA has the informal means and the contacts to
2 obtain information from other nationalities, but nothing
3 formal, and nothing enforceable. We, as I said, have
4 many formal MOUs, many informal information sharing
5 agreements, we're an active member of IOSR, which is the
6 International Organization of Securities Regulators.
7 When the NFA comes up against that border, we have been
8 able to obtain information, and here's the best part,
9 the treaties that we enter into with other nations for
10 information sharing allows us to provide the information
11 to our SROs for the performance of their routine
12 surveillance and enforcement duties.

13 So, it comes full circle. We have powers that
14 they don't have, we can use our powers to assist them,
15 and at the same time, they have the ability to fill in
16 all the gaps to do the more day-to-day stuff, the less
17 systemic stuff, and together I think it's fair to say we
18 blanket the industry and hopefully do an effective job.

19 MR. STEVENSON: Thank you, Dan. Before we go to
20 break, I would like to offer a chance if people have any
21 questions for our group of panelists here.

22 (No response.)

23 MR. CERASALE: They need a break badly, I think.

24 MR. STEVENSON: Well, we're going to give the
25 last word to Bob Whitelaw, then, before we go to break.

1 MR. WHITELAW: Hugh, if it's possible to put the
2 map up for one minute, yesterday you saw a map of North
3 America, and I just would like to point out in our
4 findings, these are advanced loans targeted, we
5 push-pinned, it's on here. We've found one interesting
6 variable that we reported immediately to the FTC, in New
7 Orleans, and in Phoenix, very few advanced loan inquiry
8 victims, negligible compared to the rest of North
9 America, and the reasons are this, and we're looking at
10 this group as to action plans and how to get right back
11 to the initial potential victim and stop it there.

12 The New Orleans paper has an advertisement every
13 day in "Money to loan, advanced fee loans or credit
14 offers, companies that do business and ask you for a fee
15 up front, that's illegal." This message brought to you
16 by the newspapers named and the FTC.

17 And in Phoenix, "Notice: Under the advanced
18 loan section, advanced loan fee brokers need to register
19 with the Arizona State Licensing Commission." Those
20 appear in the papers daily.

21 Thank you, Hugh, just for the extra moment to
22 butt in, because I'm not talking about BBB today, we're
23 talking about ways and means of awareness, and those two
24 little advertisements have probably saved a great deal
25 of heartache, heartbreak and identification theft from

1 individuals in the Phoenix and New Orleans area. And
2 the map shows why. Thank you.

3 MR. STEVENSON: Thank you, Bob, for sharing
4 that. Oh, we do have a question in the back here.

5 MR. TORRES: Frank Torres with Microsoft. I
6 agree that education can play a great role in helping to
7 avoid some of the fraud, and certainly the
8 self-regulatory programs to the extent that you can have
9 something enforceable to get to the members, to get them
10 to comply, what about the outliers? What about the
11 people that aren't or the industry groups that aren't
12 part of a self-regulatory program?

13 So, I guess my question is, how can we all who
14 are participating in the self-regulatory efforts help
15 the FTC kind of help enforce the outliers that are
16 outside of those bounds. Does that require additional
17 registration, more cooperation? I guess it's almost a
18 question for you, Hugh, is how can we be more helpful,
19 how can the DMA and others who participate in these
20 industry programs be more helpful to the FTC and other
21 enforcement?

22 MR. STEVENSON: I would be glad to venture a
23 comment.

24 MR. CERASALE: I'll take a stab at it. Frank, I
25 think one of the things that we have to do is whatever

1 group we are in self-regulation, we have a mechanism to
2 gather information. I mean, we have a complaint process
3 at DMA, others can have some other means. We don't
4 always get complaints on members, and I'm sure that
5 anyone else has that kind of a process gets some
6 outliers in a sense, and you have to try and deal with
7 them within -- we have a fairly formal process, so you
8 have kind of a due process, although we're not a
9 government entity situation, to try and get it
10 corrected.

11 If not, you then hand it over to the Federal
12 Trade Commission, or if you see that it's fraud on its
13 face, you hand it over there, or if they're in Arizona
14 and the Arizona AG or whatever. So, I think we already
15 do some of that. I think that one of the keys for us is
16 the education of people. If you have been defrauded,
17 you think somebody has, here's where you complain. And
18 they will, BBB gets information, or maybe we need
19 something, there's a whole list of places to complain
20 and try and get that going so we get more information
21 and work it through our own current processes.

22 MR. STEVENSON: Alistair?

23 MR. TEMPEST: Yes, thank you very much. I think
24 it is a very important issue, I think that there must be
25 much more cooperation between not only within countries,

1 but also between countries. And in particular, what
2 we're seeing in Europe, you've seen here, or vice versa.
3 We're going to experience things that you will find here
4 in later times.

5 So, therefore, the sort of cooperation between
6 the FTC and, for example, the European union, are
7 extremely important. The European union has just done a
8 new or is just starting a new initiative, for example, a
9 system to -- what's it called now? It's called -- I
10 have it written down here but I can't find it. Oh, yes,
11 creation of a European Network and Information Security
12 Agency.

13 Now, that's a very good idea, but obviously that
14 should work very closely with the FTC and with the
15 Canadian authorities, with the Australian authorities,
16 et cetera. We will still end up with some people
17 sitting on a Caribbean island somewhere, but then that's
18 a different question.

19 MR. STEVENSON: We'll take perhaps one more
20 question from Susan Grant.

21 MS. GRANT: Susan Grant, National Consumers
22 League. One reason why the National Futures Association
23 works so well is that membership is compulsory for
24 futures traders and it has that sort of quasi
25 governmental character. I know Canada has been or was

1 planning to experiment with forms of co-regulation for
2 certain kinds of industries where membership and self-
3 regulatory organizations would be compulsory and they
4 would have certain powers to enforce against their
5 members, and I would like an update on that, whether or
6 not that's actually taken place or whether it's worked
7 and just a reaction about that model for this kind of
8 industry.

9 MR. STEVENSON: Bob or Don, could you comment?

10 MR. WHITELOW: I can't comment on that. Don?

11 MR. MERCER: Well, certainly cooperation across
12 the border is very important. What we find in Canada on
13 the consumer's side, for example, is that we have a
14 number of organizations, a bit of fracturing in the
15 consumer organizations in Canada, which makes that a
16 little more difficult. They're more articulate and
17 correct than they are in the rest of Canada, but I don't
18 think I've really answered your question. Can you
19 elaborate?

20 MS. GRANT: I'm sorry.

21 MR. MERCER: There is a mic coming behind you.

22 MR. STEVENSON: We can pursue, but I think the
23 question was was there some move in Canada towards a
24 more compulsory membership in organizations, and I think
25 Alistair mentioned that at least in certain European

1 countries that is the case, obviously in the United
2 States that is not the case, and so --

3 MR. MERCER: I think in Canada we're not moving
4 towards compulsory membership in organizations; however,
5 when we get into the issue of voluntary codes is clearly
6 the idea that perhaps those organizations getting into
7 those codes might want to try and enlarge the number of
8 people within their tents, so to speak, to be effective,
9 and certainly that has been the case where that has
10 happened. On the other hand, enlarging membership is
11 not always a good idea, if you don't know who your
12 members are, and that has been proved in a couple of
13 cases.

14 So, I don't know whether -- I guess in some
15 cases, the compulsory aspect of membership has worked,
16 it's not clear to me that it is always of net benefit to
17 have compulsory membership in organizations. It raises
18 other questions about freedom of association, and what
19 the objectives of those members are in -- within those
20 particular organizations. I don't think it's a model
21 that we would embrace.

22 MR. STEVENSON: Thank you, Don. And I would
23 like to thank our panelists here. I think we do hear
24 some consensus on both that there is some role for
25 various kinds of industry associations, but also there

1 are some limits to those roles, and we've heard some
2 variations on how those industry associations or self-
3 regulatory organizations are set up and also some of the
4 possibilities for working across borders and using them
5 across borders.

6 So, I would like to end by thanking our panel
7 very much for participating and we will go now to a
8 short break. Thanks a lot.

9 (Applause.)

10 (Whereupon, there was a brief recess in the
11 proceedings.)

12 MR. STEVENSON: All right, I think we're ready
13 to start. For those of you tired of the old economy,
14 let's move on to the new economy. And we have to
15 introduce our Internet panelists. One of our
16 commissioners here at the Federal Trade Commission,
17 Commissioner Swindle, who has been involved in a number
18 of the international issues that we have encountered and
19 including playing a leading role in the development of
20 security guidelines at the OECD, and so Commissioner
21 Swindle has offered to make a few comments to kick off
22 our Internet discussions.

23 COMMISSIONER SWINDLE: From stage right. Thank
24 you, Hugh.

25 This is like a group of Baptists, I see

1 everybody is on the outside talking politics or
2 something, but I would like to express a good morning to
3 you and thank you for coming on a cold wintery day,
4 although it's getting to be pretty nice out here now.

5 I was in Hawaii over the weekend and could not
6 get home Monday afternoon because we couldn't land. I
7 got here on Tuesday afternoon, and got to my home, I
8 wasn't sure I would be able to do that. I got to my
9 home and had to literally dig into the house. The first
10 thing I did was plod through about three feet of snow,
11 go in and get a snow shovel, and come back out and dig
12 my way through to the house. There was a four-foot
13 drift up against the door. It was quite a shock.

14 It's a pleasure to introduce these two panels
15 which are going to focus on the role that the private
16 sector entities involved in the operation of the
17 Internet can play in helping us combat fraud.

18 Let me set the stage here by noting that global
19 electronic commerce benefits businesses and consumers
20 alike in many ways. It dramatically reduces the time
21 and cost between buyers and sellers, around the world,
22 it increases choice and convenience for consumers, and
23 at the same time it also creates new opportunities for
24 fraud. In fighter pilot lingo, this is a truly
25 target-rich environment.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

1 The issue of Internet fraud is of particular
2 concern to us here at the FTC. We have used our civil
3 enforcement authority to bring over 250 law enforcement
4 actions and against some 785-plus defendants engaged in
5 Internet fraud. But the scam artists know that the FTC
6 and our foreign counterparts still face significant
7 obstacles when these scams cross borders.

8 Internet scammers can register their domain
9 names with foreign domain registrars, they can use
10 foreign ISPs to set up websites and send spam email,
11 they can switch service providers and domain names to
12 help stay a step ahead of any law enforcement activity.

13 As you heard yesterday and today, we and our
14 counterparts have been hard at work trying to implement
15 the very strategies to fight the problem of cross-border
16 fraud, including cross-border Internet fraud, but
17 governments alone cannot do this. Public/private
18 partnerships are essential in combatting fraud in
19 general and certainly cross-border fraud related to the
20 Internet from the very systems they're associated with.

21 The recent OECD revision of the guidelines of
22 the security of information systems and networks is a
23 good example of public and private partnership working
24 well. We had representatives from industry and the
25 civil society working with and advising the U.S.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

1 delegation, which I had the honor of leading. We also
2 had representatives of both groups participating in the
3 OECD discussions. The private sector had considerable
4 influence on this effort and the final results. Because
5 of the broad public/private sector participation, I
6 believe the revised OECD security guidelines published
7 this past year are far more useful and relevant than
8 they would have been had government managed this project
9 alone.

10 I have also called upon governments and consumer
11 groups and industry to work together to create a culture
12 of security, based on awareness, accountability for our
13 conduct and taking actions that we as individuals,
14 families, firms, workers, students, teachers and
15 organizations can take to foster safe computing. The
16 same principles apply when it comes to fraud.

17 We are all involved in this, we are all in this
18 together, industry, government, civil society and the
19 public in general. We're all participants and we must
20 work together to minimize Internet fraud. This will
21 help us achieve our shared goal of a safe, competitive,
22 and a robust global electronic marketplace.

23 With that brief introduction, let me get to the
24 Internet panels. The next panel will explore the
25 circumstances under which ISPs and web hosting companies

1 can share information with law enforcement agencies and
2 help put a stop to fraudulent websites. After lunch,
3 there will be a panel on cooperation between law
4 enforcement agencies and domain registration
5 authorities. A key issue for this panel is the whois
6 database, the starting point for most Internet fraud
7 investigations.

8 How do we ensure that law enforcement agencies
9 have access to this important information? How can we
10 best work together to make sure that the information
11 therein is accurate? I encourage the panelists to focus
12 on the positives. It's important for us to discuss
13 impediments to public/private sector cooperation in this
14 area, but I would also urge panelists to try to address
15 innovative approaches to creating partnerships to
16 further our shared goal of fighting cross-border
17 Internet fraud.

18 I have never been one to readily accept why we
19 can't do something. I believe that most problems can be
20 solved, it's just a matter of focusing on it and getting
21 it done.

22 Finally, I would like to thank all of our
23 panelists. The upcoming Internet panels have
24 particularly impressive international representation,
25 including participants from Canada, the United Kingdom,

1 Germany, the OECD and Australia. The civil society in
2 the presence of EPIC is on board, and it should make for
3 a very beneficial and lively discussion, and I thank you
4 all very much. And I'll be watching on TV from the
5 floor upstairs.

6 MR. STEVENSON: Thank you very much,
7 Commissioner. I appreciate the remarks, and to pick up
8 on something that the Commissioner referred to and that
9 I know he has pressed in the security context is the
10 culture of security. In the sense here, we are trying
11 to press forward with a culture of consumer confidence
12 and to do that by developing adequate enforcement and
13 partnerships.

14 We'll turn now to the ISP and web host panel.
15 This squarely poses some of the challenges that we face
16 in a lot of our Internet cases, and we've brought a lot
17 of Internet-related cases, a lot of these have a foreign
18 component, and one of the issues is, so, how do we get
19 the information we need to go from stop to go and
20 actually bring the case?

21 I thought what we would do here to start is have
22 Eric Wenger, who is from our Division of Marketing
23 Practices and has been involved in a number of the
24 important Internet cases that we've brought, describe
25 from the enforcer's perspective where we start. Say you

1 know that there is a website or an email that's the
2 problem, well, where do you go from there? How do you
3 get the information, what issues do you encounter in
4 dealing with the Internet infrastructure and how do you
5 address that? So, we'll start by having Eric make a
6 couple of comments about that and then turn to our other
7 panelists.

8 MR. WENGER: Thank you. Because of the
9 privatization of the Internet, it is vital for us to get
10 information from the private sector when we're
11 conducting law enforcement investigations. So, where we
12 start typically is with the website. Let's say, for
13 example, that it has some suspicious elements to us, and
14 we want to figure out who may be responsible for it, so
15 we can evaluate whether or not we want to take some sort
16 of law enforcement action.

17 So, as Commissioner Swindle noted, the first
18 place we start, typically, is with the whois database.
19 And so, for example, I've put up on the top left screen
20 there, a screen shot from one of our cases that involved
21 a fake Yahoo page that was supposed to be a sweepstakes,
22 and it lured people into downloading software that
23 caused them to incur very high telephone charges, \$2.99
24 a minute over a 900 number line. Which they were told
25 was necessary in order to claim a prize that didn't

1 actually exist.

2 In any case, in this example, the first thing we
3 would do is to look up in the whois database to see who
4 is the registered owner of the website, and the subject
5 of the information that's in the whois database, which
6 I'm sure you all know is freely available, and how
7 accurate that information is, will be the subject of a
8 later panel, but suffice it to say, if that information
9 is accurate, it's very helpful to us, because it allows
10 us to identify who it is that is the registered owner of
11 the domain name for the website.

12 And if we had the ability to search the
13 database, for common elements, like addresses or
14 telephone numbers, or email addresses, we would be more
15 likely to be able to locate common websites that are
16 registered to the same person. So, that's also an issue
17 for us is once we've identified who might be the
18 registered owner of a domain name, if we can identify
19 the scope of the problem, what other websites they may
20 have, it would help us to evaluate the strength of our
21 case.

22 And then there are typically two pieces of
23 information that we would look for from other companies
24 that we know through the whois database. We typically
25 would be able to identify the registrar for the domain

1 name, and also a web hosting company. This particular
2 example, there was not a separate domain name that was
3 registered, but assuming that there was, we would turn
4 to the registrar and ask them if they had information
5 about the source of payment for the domain name, and
6 also if they had captured any electronic information at
7 the time of the set-up for the domain name, such as an
8 IP address.

9 And the same would go for the web hosting
10 company, we would turn to them and ask them if they had
11 payment information that would give us a money trail and
12 also if they had collected some sort of Internet
13 protocol address that would hopefully get us back to the
14 person or persons or entity that set up the webpage.

15 Of course, there is in these cases, we use
16 subpoenas, because the registrars would require them and
17 the web hosting companies or Internet service companies
18 were required to use them under the Electronic
19 Indications Privacy Act. But that's the basic structure
20 of what we're looking for. And that's probably it.

21 MR. STEVENSON: Well, suppose the information in
22 the whois database may be inaccurate, you're relying on
23 the information from the web host in this case to track
24 who is behind the website. What happens if you can't
25 get that information? If you can't trace back through

1 that line?

2 MR. WENGER: We do try to trace the sources of
3 payment as a mechanism. We try to deal with consumer
4 complaints to figure out if they have information about
5 who they may have paid, but the electronic information
6 is vital to us, and if we can't get it because the
7 information was never logged, or we can't get it because
8 the information was logged but was deleted before we
9 were able to get to it, or if we can't get to it because
10 the company that has the information will not abide by
11 our request for confidentiality, then that avenue of
12 investigation is dried up for us, and it becomes a major
13 problem.

14 MR. STEVENSON: Okay, so speed is important in
15 response, and confidentiality is important, I take it,
16 maybe you could just say a few more words about that.

17 MR. WENGER: The investigations that are
18 conducted by the Federal Trade Commission are required
19 to be nonpublic, and so if I go to ask a web hosting
20 company or an Internet service provider for information
21 about a subscriber pursuant to a subpoena, and they say
22 to me, we'll give you this information, but we're going
23 to notify the subscriber, that might be an impediment
24 that would make it impossible for us to get the
25 information from that source, because it would disclose

1 the existence of the investigation, and that's something
2 that we're not permitted to do.

3 And the timing issue is also very important. As
4 you mentioned, if I want to trace from a website to a
5 user, there are a number of different layers that I have
6 to go through.

7 If I go to the web hosting company and they give
8 me an IP address that leads back to an Internet service
9 provider, then I need to tie that back to a user
10 account, and hopefully to the actual user's computer,
11 and that may require me to go first to the web hosting
12 company, then to the Internet service provider and then
13 possibly to the telephone company, and if each of those
14 steps takes too long, then the data, even if it was
15 recorded, might be gone. Or if somebody won't abide by
16 our confidentiality request, then I might not be able to
17 get to the level of information I need in order to trace
18 the activity back to the person who is perpetrating it.

19 MR. STEVENSON: Thanks, Eric.

20 Let me now turn to a couple of our panelists.
21 Let me make sure they're here. Sarah Deutsch from
22 Verizon, sorry, and ask you just to maybe respond first
23 to the basic scenario that Eric has laid out here in
24 terms of responding to a domestic enforcer, say the FTC,
25 and then what additional complications there might be if

1 it's, for example, the ACCC, the Australian Competition
2 and Consumer Commission.

3 MS. DEUTSCH: Sure. I guess, you know, Verizon
4 cooperates daily with law enforcement on a whole variety
5 of matters, and we feel very strongly that we have to
6 work to eliminate Internet fraud, both to protect
7 innocent people, but also to bolster user's confidence
8 in the Internet. In this case, the FTC's power to go
9 after people flows from its police powers, and you do
10 have I guess an administrative subpoena that you get to
11 serve on service providers, and we're there to help you.

12 One of the cases that you've probably heard
13 about that's garnered a lot of media attention, and that
14 would I think actually result in more consumer fraud, is
15 when that same police power to issue a subpoena comes
16 from a private party, and that's been the case when the
17 recording industry has sued Verizon, essentially that
18 case would grant any private person the right to fill
19 out a one-page form, send it to the service provider and
20 get someone's identity, again, based on the same IP
21 address that the FTC uses.

22 We're very concerned that this would actually
23 result in more consumer fraud, because anyone will be
24 able to get your identity, and at that point, if they
25 want to perpetrate fraud on you, they have the key to

1 unlock your identity. So, we're very concerned with
2 that issue.

3 That being said, I think there are some
4 additional problems when the subpoena is coming from an
5 agency outside the U.S.

6 Hugh, is that also your question?

7 MR. STEVENSON: Yes, it is.

8 MS. DEUTSCH: Okay.

9 MR. STEVENSON: And I apologize, I did not
10 mention as a special guest star on the panel, we
11 actually have one of the commissioners from the ACCC,
12 Sitesh Bhojani, who also joined us yesterday, and maybe
13 he then could comment on your comment.

14 MS. DEUTSCH: These are some of the problems
15 that we've identified. I guess first of all, it's not
16 clear that service providers have the authority to
17 respond to a request from a provider or an agency
18 outside the U.S. without some sort of mutual legal
19 assistance, treaty or some other statute that requires
20 that we comply.

21 I think right now in our own law, there's a
22 provision in 18 USC 1703 that allows us to provide
23 subscriber information in a law enforcement
24 investigation for telemarketing law, but we don't think
25 this extends to foreign law enforcement investigations,

1 because the way we see this defined in U.S. law is
2 applying to only domestic agencies.

3 So, there's a question, I guess, as to whether
4 we need a treaty and/or a statute in order to be able to
5 comply more fully.

6 I think there's also a question about what is a
7 fraud? We face this in the Council of Europe Cyber
8 Crime Treaty that there are acts here in the U.S. that
9 could be legal but are illegal overseas or vice versa.

10 For example, in Germany, comparative advertising
11 is illegal, or Land's End offering a money-back
12 guarantee for merchandise was considered an unfair
13 marketing practice. So, you know, there needs to be
14 some discussion of what would be a fraud, and I guess
15 those are some of the main issues and we can get into
16 the details later.

17 MR. STEVENSON: Okay. Commissioner Bhojani,
18 maybe we could ask you to comment. Say we have the
19 hypothetical of you needing to investigate a scam and
20 needing to track back who is behind the website.

21 MR. BHOJANI: In an international context or in
22 a domestic context?

23 MR. STEVENSON: I'm sorry, and let's assume that
24 the web host or ISP you're dealing with is in the United
25 States.

1 MR. BHOJANI: Yeah, that really has been -- we
2 actually have experienced that sort of issue. It really
3 has been relying on voluntary cooperation, I don't know
4 that there is any power, I think what Sarah said is
5 probably right, that there isn't any legal authority on
6 which that sort of action can be undertaken. And so
7 there is a little bit of an impediment in that sense,
8 although we have had, as I say, some success just on a
9 voluntary basis with various ISPs willing to provide
10 that sort of information or whois database information
11 as well.

12 What I'm curious to hear about is whether there
13 is any grounds that Sarah thinks perhaps the fact that
14 the commission, the ACCC may have instituted court
15 proceedings in Australia might give you sufficiently or
16 reasonable grounds to give us some of the information or
17 to suspend services or things of that kind.

18 MR. STEVENSON: Sarah, do you want to respond?

19 MS. DEUTSCH: Yeah, I mean, I think we should
20 clarify that if we get any request or alerting us of any
21 fraud occurring somewhere on our system or network, we
22 take a look and if we see something is wrong we try to
23 do something about it, we'll either pull down the site
24 or notify law enforcement.

25 So, we do want to cooperate, but I was kind of

1 looking at the bigger legal issues of what we would need
2 in order to kind of create a more efficient process for
3 dealing with some of these issues more globally.

4 MR. STEVENSON: Chris Bubb from AOL, maybe I
5 could ask you for your sort of reaction to this, because
6 I know that you all have had a lot of occasion to deal
7 with requests from all over the world.

8 MR. BUBB: Yeah, we deal with international
9 requests on a fairly irregular basis. Normally the
10 international requests are based on the Mutual Legal
11 Assistance Treaty process that's out there for criminal
12 investigations. I mean, the actual name is misleading,
13 it's not mutual legal assistance, it's mutual legal
14 assistance in criminal investigations. So, it's limited
15 to criminal context, but we do have a lot of
16 relationships with investigations from other countries.

17 One of the things we've found is that it's often
18 useful to use the [FBI] LEGAT in the embassies in the country
19 that is requesting the information, where the FBI has
20 LEGATS and there are other LEGATS in various embassies
21 where they can act as an intermediary and get the
22 information and then pass it on to the law enforcement
23 or requesting agency and the requesting country.

24 Because the Mutual Legal Assistance Treaty
25 process is a lot more efficient than it used to be, the

1 letters rogatory and the other processes that you had to
2 go through were very cumbersome, but the MLAT is not
3 exactly a model of efficiency in terms of dealing across
4 borders, and countries are very jealous about their
5 sovereignty and their jurisdiction, and they're not
6 inclined to bend that at all, and that's why the mutual
7 legal assistance is required.

8 I did some research in preparation for this and
9 I actually found out that there are some interesting
10 possibilities out there for action, I think the FTC has
11 been a ground breaker in the antitrust investigations
12 and have put together a regime called the International
13 Antitrust Enforcement Assistance Act, and then they
14 issue what they call antitrust mutual assistance
15 agreements, bilateral agreements, because of this, they
16 ran into the same problem, which was MLATs were
17 criminal, and in many countries, the antitrust issues
18 are civil and taken care of by civil authorities, and
19 they couldn't get around the MLAT issue.

20 So, I think there may be a model there for
21 dealing in a fraud context, to establish bilateral
22 arrangements. It apparently has also happened in the
23 securities and exchange, where they have identified, for
24 instance a major fraud, and then they would engage in a
25 memorandum of understanding between two countries for

1 the exchange of information under certain circumstances.

2 And I think that would be useful as a framework,
3 or something like that might be useful as a framework
4 for dealing with the civil law enforcement issues in the
5 United States, and what we deal with mostly, which is I
6 guess the back door, but the Australian issue, which is
7 all of our information, or 99.9 percent of all the
8 information that AOL has is resident in the United
9 States, and all of our relationships with foreign law
10 enforcement have been requests to us for information for
11 a what we would call foreign or non-American request.

12 MR. STEVENSON: Chris, let me ask you a
13 follow-up question on that, because I think the larger
14 point is a very interesting one to us in the interest of
15 looking in the securities and antitrust context for
16 mutual assistance agreements, but let me, and I think
17 Eric, maybe on your other slide, maybe this was clearer,
18 these sort of timing challenges here.

19 MR. BUBB: Oh, absolutely, right.

20 MR. STEVENSON: And maybe if you could address
21 that, and I have a weak grasp on this, but my
22 understanding is the problem is that you got some of the
23 information that you need to track back to the machine
24 is just session IP address information, and so it's only
25 good for a short period of time, and so if you don't get

1 it quickly, you sort of lose your chance to get the next
2 step back in the chain.

3 MR. BUBB: Right. Absolutely. The issues are
4 all generated by the magnitudes of scale that we deal
5 with, at least in America Online. It's true of every
6 Internet service provider within limits, but America
7 Online is strictly based on a dynamic ISP. We assign an
8 ISP to a user per session, and when the user
9 relinquishes that IP, for whatever reason, whether he
10 signed off or whatever, if he relinquishes that Internet
11 protocol address that we have assigned him, that
12 protocol address is available again for assignment to
13 the next user.

14 We have 35 million members and the ability to
15 have approximately three million simultaneous users.
16 So, that means only one in ten people would, you know,
17 at any given time be on, and so what we're talking about
18 is a dynamic system, so it's temporal, it's time-based.

19 And we keep them for varying amounts of time,
20 the information for varying amounts of time. We have
21 emails, we deal with over a billion emails a day, over
22 13 million web hits a day. So, all of that information
23 is collected and kept for varying periods of time,
24 depending on the requirements of the company in terms of
25 recordkeeping.

1 And so, we have retention issues in terms of
2 that information. And it's extraordinarily important
3 for law enforcement of any kind to come to us in a
4 timely manner to get that, because it's sort of like
5 Lucille Ball with the cherries going down the conveyer
6 belt. You know it's going to fall off, it's going to
7 drop, and no matter how hard Lucy tried to collect all
8 the cherries, she couldn't do it, and nor can we.

9 There are some mechanisms that are very useful.
10 There is a preservation request letter under 2703(f)
11 where we will freeze that information in time and put it
12 aside for law enforcement further requests, but even
13 that has to be done in a timely fashion.

14 MR. STEVENSON: And let me follow up on that,
15 because I think Eric or Lucy or Ricky or whoever told me
16 that one of the challenges there is not the issue of
17 getting you to preserve it, it's sort of to get the
18 entity behind that to preserve it. And actually, Eric,
19 if you want to just mention what we had sort of
20 discussed about your concern there.

21 MR. WENGER: Sometimes what happens is that
22 there's an Internet service provider and then they use
23 somebody else to provide telephone connectivity, and for
24 instance I think AOL has companies that provide the
25 modems in each of the cities, and so we need you to

1 preserve the information you have and then also there's
2 a challenge of getting it back quickly enough in order
3 to get a preservation request to whoever is providing
4 that actual modem.

5 MR. BUBB: Right. All of AOL's dial-up
6 operations are contracted out to one of five or six
7 dial-up providers, including WorldCom, Sprint, companies
8 like that. And you're absolutely right, that the only
9 chance you have of getting to the actual, in your
10 scenario, the user location, the telephone or the home
11 that it's coming out of, would be a two-step process
12 with America Online, to get our information and then to
13 get the information that we have that leads back to the
14 dial-up provider.

15 We do that, and as a matter of fact,
16 interestingly enough, when we do it, when we provide the
17 information back again, we give a cheat sheet along with
18 it, as well as the whois information for the dial-up
19 provider and the contact telephone number. So --

20 MR. WENGER: I guess I'll put this out to any of
21 the Internet service providers. If there's a situation
22 where there may be somebody downstream from you that we
23 may need to get information from, would it be possible
24 for us to give you a preservation letter that would
25 cascade, in other words you would send it immediately to

1 the secondary preservation, in other words, we wouldn't
2 have to wait to get back your information and then get a
3 second subpoena.

4 MR. STEVENSON: Another way of thinking that, on
5 a voluntary basis, is there a way to get at least so the
6 information is preserved immediately, even if it can't
7 be obtained immediately?

8 MR. WENGER: We would of course have to issue
9 the subpoenas to both companies to get the information.
10 But if it would turn out by the process of issuing the
11 subpoena and getting a response from the first company
12 would take so long that the second company would no
13 longer have the data, the question is exactly as you put
14 it, is there a way to preserve everything downstream,
15 just preserve the status quo in a way that allows us to
16 in the course of time issue the subpoenas and get the
17 information.

18 MR. BUBB: Well, I guess it wouldn't be a
19 problem, the only practical observation I make about
20 that is that when we process the information, that's
21 when we know who the downstream provider is. So, we
22 wouldn't know it until we process it. So, we wouldn't
23 be able to say that it was UUNet or Sprint or Genuity.

24 So, it adds a complication to it. I hadn't
25 thought about it, I don't imagine there's a huge issue.

1 What we could do informally is to notify the downstream
2 provider that we had gotten the request, and ask them to
3 take the steps they need to take relative to it on an
4 informal basis. I don't think we would do it formally.
5 I mean, we would ask for it, because I don't think we
6 would be, I don't know, I guess I don't know what the
7 legal term would be, but really in a position to demand
8 that they do it, but I don't have a problem with an
9 informal request saying that we had gotten this, it's
10 connected to you, would you look to preserve.

11 Or the other thing would be as soon as you get
12 the information, I mean you would get it roughly about
13 the time that we got it, immediately issue a request for
14 preservation to them. Our dial-up information, I guess
15 on the other side of it, is among the more durable
16 records that we have. It's the longest one, amongst the
17 longest retention tables that we have. But that's a
18 side issue.

19 MR. STEVENSON: I don't know whether Sarah or
20 Kristen wanted to reply to that particular point.

21 MS. DEUTSCH: I mean, for us it's a very
22 relatively small ISP compared to America Online. We're
23 also not a backbone provider. I think the issue will
24 come mostly for the backbone providers and the key here
25 would be getting you enough information as quickly as

1 possible so you know who this downstream provider is and
2 you can get this request to them as soon as possible.

3 MS. VERDERAME: If I answer this question, it
4 opens a whole host of other issues that I am not going
5 to get into at the moment. In the European system, it's
6 quite different from over here in many respects. One of
7 the issues is that privacy over there is actually a
8 human right, so it's very highly protected. The data
9 regime over there is very severe and very strict. So,
10 any kind of disclosure, whether it's to law enforcement
11 or anyone, is severely limited.

12 The European data protection directive under
13 which we have to work also requires mandatory
14 destruction of data. So, if you're talking about going
15 in and wanting to find certain information that's there,
16 if it's already been destroyed, there's an issue.

17 In direct answer to your question, what I would
18 say is that we have very good relationships with the
19 ISPs that we serve through our content hosting business,
20 and also as an ISP with our customers. We have
21 contracts that cover this exact type of situation, if an
22 issue arises, we can terminate service immediately, with
23 no notice. We work very closely with law enforcement
24 and are happy to work, even on an informal basis,
25 contacting the ISP with whom we're serving through our

1 content hosting business, or the customer directly or
2 whoever it might be, downstream, to try to preserve
3 information.

4 If there's no legal requirement to do so, we
5 can't force their hand, but we have been known in the
6 past to do that, to work cooperatively with folks to try
7 and preserve what law enforcement is interested in
8 seeing.

9 MR. STEVENSON: Kristen, let me just pose the
10 scenario, maybe this is the reverse of the one we were
11 talking about earlier where the -- say the Australian
12 consumer protection folks are trying to get information
13 from an American web hoster ISP, and so the sort of
14 different scenario is say where the FTC or the ACCC is
15 trying to get information from a European-based ISP. I
16 mean, how does that look in terms of your ability to
17 respond? Is your answer different from Chris', or how
18 is it different? Obviously you've suggested already
19 it's different.

20 MS. VERDERAME: It's not different as far as
21 legal procedure goes. We have the same concerns as far
22 as desiring some sort of international treaty to give
23 the entity the authority to come in and get that
24 information from us, but we also have to overcome the
25 data protection restrictions and requirements that we

1 have to fulfill there. We certainly have an expert on
2 the panel who can speak to that more than I, but that is
3 a definite hurdle that we have to overcome is the data
4 protection regime.

5 MR. STEVENSON: Eric, I think you had a comment
6 following up on that.

7 MR. WENGER: The flip side to the scenario that
8 I proposed before is where, for instance, there's a web
9 hosting company that gives me back and I give him a
10 subpoena and they have an IP address that comes back to
11 one of the ISPs on the panel here. Would they be
12 willing to accept a confidentiality request that comes
13 upstream from you, absent -- in order to avoid the
14 situation where I have to, again, wait for the response
15 to come back from that other company, and then issue a
16 preservation letter to you during which time the data
17 that I'm looking for might evaporate?

18 MR. STEVENSON: And Eric, maybe it's helpful for
19 you to talk about the time frames that you've
20 encountered in terms of how fast you need the
21 information.

22 MR. WENGER: For example, in something that I'm
23 currently working on, there was a web hosting company
24 that gave me -- I issued a subpoena, it takes about two
25 weeks from the date that we have a subpoena issued for

1 the responses to come back, and then I get back an IP
2 address from them that comes back to a particular
3 Internet service provider. And I say to them, I want to
4 know which of your users was assigned to this IP address
5 at this date and time. And they tell me that their
6 record retention is only for about seven days.

7 So, the process of just the response time for my
8 subpoena exceeds the length of time that the data is
9 retained for. And I understand the sensitivity, I think
10 we all do at the FTC, about just having data retained
11 forever, because there are cost concerns and there are
12 privacy concerns, but our concern is that where we have
13 narrowly targeted requests for information, that it be
14 retained and disclosed, are there ways to make sure that
15 the information is there when we need it?

16 MS. DEUTSCH: Well, I think you've got a very
17 legitimate concern. I mean, Verizon keeps the session
18 logs for a very long time. I mean, months, you know, in
19 some cases years later you can get from us, you know,
20 the user ID, their phone number, address, the date and
21 time stamp that this was happening. I think we need to
22 push for some best practices so that these kinds of
23 records can be kept in a manner in accordance with the
24 usual business practices that also, you know, serves the
25 needs of the law enforcement community, but that's that

1 we feel strongly that it's still preserved.

2 We would prefer a data preservation model versus
3 a retention model, but for these types of business
4 records, I think we should, you know, try to work toward
5 better practices so that you can get the information you
6 need.

7 MR. STEVENSON: Is it fair to say that the --
8 because one issue we've heard raised in many larger
9 contexts of obviously it's a burden of retaining just
10 this information in general for a long time. Is it fair
11 to say that to the extent there could be developed a
12 mechanism for targeting smaller amounts of information
13 to be preserved, that that is maybe a useful direction
14 to go in terms of our ability to investigate these
15 cases?

16 MR. BUBB: I think that's exactly the model
17 that's preferred. Just again, I always like to view
18 these things in context, and one of the contexts is in
19 some of the dynamic IP addresses that we deal with, and
20 I won't go into the technical ones, but one set of
21 servers at America Online generates between seven and
22 nine terabytes a day of information relative to certain
23 IP addresses. I mean, that's just an enormous amount of
24 information to preserve to hold onto. And it starts
25 to -- the answers to the questions that are posed start

1 to be practical answers rather than, you know, sort of
2 theoretical answers.

3 The practical answer is there's only a certain
4 amount of space that you have to store between seven and
5 nine tarabytes, you know, we're having to learn whole
6 new vocabularies of the next thing up from a tarabyte.
7 So you're really starting to look at massive amounts of
8 information. And we preserve actually a lot of it.

9 I think the second thing that needs to be
10 observed is that there are two things. One is the
11 information, the second one is the ability to resolve
12 that information down to an individual user. And a lot
13 of times, at AOL, we go out of our way, and it's a part
14 of our own business, not in order to assist anybody, but
15 we retain the ability to resolve it down to individual
16 users over time. A lot of times, there are vast amounts
17 of information that are kept and logged, but they are
18 not able to be useful to any law enforcement agency that
19 would come to you, because they're just a mass table of
20 IP addresses.

21 So, that's a secondary thing that one has to
22 keep in mind with web hosting or anything else is
23 whether that information that is kept is capable of
24 being tied to anybody, to being resolved back to or
25 pointing to anybody.

1 So, that's just a secondary issue.

2 MR. STEVENSON: Okay. Thank you.

3 Well, and so both the challenge is to tie it to
4 someone, but then that also raises some of the privacy
5 concerns that Kristen raised. I guess I would turn next
6 to Jonathan Bamford and ask is Kristen's assessment
7 basically correct, then, and how should one look at
8 this? How can one get this done consistent with privacy
9 concerns?

10 MR. BAMFORD: Well, Kristen is not far off the
11 mark in terms of the fact that you do need to be
12 concerned about data collection legislation, and perhaps
13 because perhaps we are two nations divided by a common
14 line, I ought to actually explain what data protection
15 legislation is, because it's not some overarching
16 absolute right of privacy.

17 It is based on, to a certain extent, the
18 European Convention of Human Rights and individual
19 rights to a private life, but even that is not an
20 absolute right and that can be interfered with certain
21 circumstances in accordance with the law and in a
22 proportionate manner to the evil you're trying to
23 address there.

24 So, clearly, there's a balanced approach in a
25 sense of respecting people's private lives, and actually

1 protecting the States against criminality over
2 individuals against criminality against them. Or of the
3 fraudulent activities. So, it isn't an absolute right.

4 I mean, in common with many, many other
5 countries around the world, not just European Union
6 countries, but Canada and Australia also have data
7 protection legislation that sets down some legally
8 enforceable standards in terms of the collection of the
9 information. Most individuals understand when they're
10 providing information, how it's used, how it's
11 disclosed, data quality standards regarding accuracy and
12 the things that have been searched done elsewhere and
13 searches as far as the accuracy of data and also
14 security.

15 The thing I would stress to you is that data
16 protection legislation only actually relates to
17 identifiable living individuals. There's no protection
18 for companies or anything like that. Or aggregated data
19 or anything along those lines, it's only where it
20 actually points to an identifiable living individual.

21 And I think it's important to understand as well
22 that it does apply to both public and private sectors in
23 most jurisdictions as well. It also provides some
24 protection for individuals as well in terms of rights to
25 access and things like that, which perhaps we don't need

1 to go into today. And also one key feature of the data
2 protection legislation is that you have to have an
3 independent supervisory authority, and that's the
4 Information Commission of the United Kingdom and all
5 jurisdictions have their own supervisory authorities.

6 And we try and work in a constructive way to
7 deal with the very issues that you're raising there,
8 Hugh, in terms of providing people with the appropriate
9 advice in terms of how data protection legislation
10 applies. And sometimes there is the immediate reaction
11 that, hah, data protection legislation applies to some
12 information about some individual that's being sought
13 here, therefore you can't have it. That would be a
14 wrong approach to adopt.

15 Data protection legislation usually has certain
16 balancing features in it. Indeed, sometimes you can
17 disclose information just because you've made people
18 aware at the time that they signed up to be your
19 customer, how you are going to use and disclose their
20 information. Not particularly relevant when we talk
21 about whois databases in certain instances and
22 relationships with ISPs in terms of how widely that may
23 be made available, indeed to the law enforcement
24 community, in its wider sense.

25 But a lot of the questions that you've got to

1 ask in data protection terms is centered on the nature
2 of the data being sought. I think there were some
3 relevant questions starting to be posed yesterday that
4 were described as meta data, but what actually we are
5 talking about sharing here, although I have to say I'm
6 not quite certain it's always sharing as a disclosure of
7 information, it's giving information. Sort of my kids'
8 definition of sharing I think is probably used,
9 actually. But they get everything and never share it
10 with their sisters.

11 But, basically, you know, it's a question of
12 what's being sought. And there's clearly differences
13 there between an actual investigation into somebody who
14 is a suspected perpetrator of a crime and perhaps other
15 information which is generally about customers to help
16 identify crimes, trends or other things which may
17 suggest they have been subjects of the crime where
18 actually they haven't done anything wrong and there's
19 different responsibilities there.

20 Within our data protection laws, we often have
21 exemptions from what we call our nondisclosure
22 provisions, which restrict disclosure, where failure to
23 disclose would be likely to prejudice the prevention or
24 detection of crime or the apprehension or prosecution of
25 offenders. There are some issues on the merging of

1 what's an offense and what's not an offense, but there's
2 a mechanism there, our policing in the UK hasn't simply
3 grounded to a halt since we've had data protection
4 legislation since 1984.

5 They can find out information about people
6 because they request it on the basis of its likely to
7 prejudice the prevention or detection of crime, and
8 people then faced with that request, whether it be my
9 Internet service provider, who happens to be BT Internet
10 by some chance there, and but, you know, they would
11 weigh a question in terms of would it be -- do they have
12 reasonable grounds for believing it likely to prejudice
13 crime prevention purposes.

14 Similarly, if they're under a legal compulsion
15 to provide legal information as a result of a court
16 order or some direct legal power, they can do that
17 without violating data protection laws. There's wider
18 issues we're touching on here about the applicability
19 and the legally binding nature of a court's orders from
20 other jurisdictions or other powers of body there, which
21 maybe we'll come back to, but there are mechanisms in
22 legislation which permits disclosure in certain
23 circumstances.

24 MR. STEVENSON: Let me ask you in terms of the
25 scenario of one issue in response to a legal process,

1 but for example, take my scenario where the ACCC is
2 investigating somebody who needs to go to British
3 Telecom to get information. Does that pose a problem?

4 MR. BAMFORD: Well, the first instance, if I was
5 in British Telecom's shoes, I would be asking who the
6 heck are the ACCC, which might not be actually be known
7 to many people. No disrespect there. And perhaps other
8 people in the UK that would ask that of the FTC as well
9 because they wouldn't know. I'm sure you're very, very
10 well known over here, but we don't know who we're
11 dealing with in many instances. If you're in that
12 position.

13 So, how do you know that it's a legitimate
14 request from a law enforcement agency? And that's the
15 real difficulty. I don't know how somebody would react
16 if they got a request from the Hazzard County Police
17 Department, I don't know whether that's a legitimate
18 police force or not.

19 It's difficult. And I would actually say a
20 better model, and we're here talking about partnerships
21 in the title of this conference, is to have a designated
22 contact point within that jurisdiction with the
23 appropriate powers. It's the conduit of finding the
24 information, because the people locally are used to
25 dealing with those, they know them as a law enforcement

1 agency, and they can be the appropriate conduit back.

2 Within the UK, we're doing things to try, it
3 tends to be in the criminal law areas, but we have a
4 bill going through Parliament at the moment which is
5 essentially a crime international cooperation bill,
6 which is all about one serving process, clearly people's
7 responsibilities in terms of obeying, that's a rather
8 difference in a jurisdiction where you can't enforce it,
9 but two, assist in investigations to provide the
10 necessary information.

11 So, we're trying to bring about a system of
12 greater cooperation. That brought to bear in the data
13 protection context, if a local law enforcement agency
14 perhaps has requirements for somebody to provide
15 something, such as our Office of Fair Trading, then that
16 would be the conduit back.

17 And I would make the point as well, that
18 presumably because we're talking about the Internet
19 here, and therefore the crime can be committed against
20 consumers anywhere in the world, there may be well some
21 local jurisdictional issues as well, if the suspects are
22 operating in the UK, that they are actually committing
23 crimes against UK consumers and they have a legitimate
24 law enforcement interest of their own, which again gives
25 greater weight to a disclosure by an ISP based in the

1 UK. It's a local law enforcement concern.

2 MR. STEVENSON: Let me follow up on two things
3 there. One, I wanted to see if I understood correctly
4 one of your suggestions, which is that the ISPs may be
5 able to address some of the privacy concerns in terms of
6 service, in terms of disclosure of what might be done
7 with the information? Was that one?

8 MR. BAMFORD: It's a possibility of doing that.
9 I mean, I think it would depend on the nature of the
10 data and whether there would be some unfairness to
11 individuals. Clearly when there's a situation where
12 there's a complete legitimate concern about somebody,
13 you know, and there's real issues about their compliance
14 with the law, you perhaps are less dutious to them in
15 terms of fairness and how you process their information,
16 than you would about people who are potentially
17 completely blameless.

18 And so it would depend upon the nature of the
19 data that's being sought, the extent to which you could
20 rely on a contractual term, but it's not so unusual as
21 you will see when we talk about whois, to see in
22 contractual terms the fact that this information will be
23 disclosed to bona fide law enforcement agencies.

24 And I think you'll all find as well as a result
25 of an agreement between the EU and American authorities,

1 airline passengers are being told how their information
2 will be available to U.S. authorities, and now if you
3 read USA Today on that particular agreement.

4 MR. STEVENSON: I think that's an interesting
5 point to think about. The other issue that you raised,
6 Jonathan, was the issue of working through the local
7 authority, the local enforcement authorities, local from
8 the point of view from I guess the ISP or the web
9 hosting company, and I'm wondering whether anyone had
10 any reaction to that. Does that make sense to -- maybe
11 the better way is to say, that makes sense, doesn't it?
12 Or is there a particular reaction? Or is there a
13 different model?

14 MS. VERDERAME: Well, I would add that that is
15 correct, and that's the method that BT certainly uses.
16 That's sort of our first port of call.

17 If I could just make a couple of comments.
18 First of all, I would say that earlier my intention in
19 stating or raising the data protection regime was not to
20 say that it prevents us from disclosing information to
21 law enforcement and that sort of thing, just to strike
22 the difference between the U.S. and the UK. We don't
23 have that over here, we do have that to think about that
24 over there. In fact, when I surveyed a lot of our folks
25 with questions for this panel, one of the first things

1 out of their mouth was data protection, we have to think
2 about that first.

3 So, we're actually grateful to have the
4 information commissioner's office to go to when there is
5 an ambiguous area. Certainly we have a process in
6 place, when things come in the door, we have people
7 dedicated to look at the subpoenas or whatever they
8 might be, they're familiar with the ACCC and other
9 authorities around the world, so we have a process in
10 place and it does include, in fact, law enforcement on
11 that.

12 MR. STEVENSON: Thank you. I would like to turn
13 now to Cedric and ask for his reaction as someone who
14 focuses on privacy issues and I'm wondering whether the
15 scenarios that we've described and that Eric described,
16 what kinds of issues that raises from your point of
17 view, what concerns, what ways are there of addressing
18 them?

19 MR. LAURANT: I would like first to re-focus the
20 debate a little bit, because so far, we've talked about
21 how data protection, how privacy laws may be hurdled to
22 law enforcement work, and especially the law enforcement
23 work of the FTC. But I would like to remind you that
24 the FTC is, first and foremost, a consumer protection
25 organization whose main task is to protect consumers

1 from fraud, from identity theft, et cetera.

2 The second point I would like to make is that
3 law enforcement has its own interest in, for example,
4 suing criminals, suing identity thieves, et cetera, and
5 then consumers have privacy interests. So, you have to
6 take into account on the one side, law enforcement
7 interests, and on the other side, privacy interests.

8 We at EPIC, Electronic Privacy Information
9 Center, of course are more focused on privacy issues and
10 on protecting, on raising labor issues and price issues
11 and trying to understand how consumers can get their
12 privacy better protected. And I think that the role of
13 the FTC as a consumer protection agency is to take into
14 account in balancing the interests of, on one side, law
15 enforcement interests, and on the other side, privacy
16 interests. And having this framework in mind, I think
17 we should think about, because we are on a panel trying
18 to understand how law enforcement and private sector
19 could better cooperate among each other, with each
20 other.

21 I think we should try to understand why there
22 may be impediments to the sharing of information. Those
23 impediments probably exist between, for example, the
24 United States and the European Union, because the
25 European Union promotes data protection as a human right

1 that is protected by the European -- mainly by the
2 European Convention on Human Rights, in its article 8.

3 And taking this into account, a way to have
4 better partnership between a private and law enforcement
5 and public agencies would be to have kind of general
6 framework, general data protection framework that could
7 be incorporated into the various memoranda of
8 understanding or intellectual agreements that are now
9 being signed between countries like Australia and the
10 U.S., United Kingdom and the U.S., and Great Britain and
11 the U.S., and such a framework could actually be the
12 OECD privacy guidelines, so the Organization for
13 Economic Corporation and Development privacy guidelines.

14 Let me remind you that the FTC has always been
15 very active, first of all, in drafting these guidelines,
16 and then in recognizing them as a good model to protect
17 consumers, especially through the fair information
18 practices.

19 So, we at EPIC would view the OECD privacy
20 guidelines as a good supernatural framework to protect
21 consumers' privacy, and we think that it should be
22 incorporated into the various international agreements
23 that would promote better cooperation between law
24 enforcement authorities and private companies, and
25 consumer agencies.

1 MR. STEVENSON: Thank you.

2 Let me follow up on part of that comment.
3 Obviously one of the things that needs to be addressed
4 is some understanding across borders of how these things
5 might work. There is an Australian example, and maybe I
6 could ask Mr. Bhojani to address, but I think it's
7 particularly the ASIC, sort of the Australian version of
8 the SEC, has been involved with in terms of voluntary
9 codes with the ISPs. It's just sort of an interesting
10 project that perhaps if I could ask you to just describe
11 that briefly and ask whether that has the potential of
12 broader applicability.

13 MR. BHOJANI: Thank you, Hugh.

14 Yes, if I could put the issue in a bit of a
15 context, most of you, I think, have probably had a
16 handout given to you about the sort of Australian
17 Communications Authority, which is not us, obviously,
18 but one of our sister agencies who's responsible in this
19 area, have put out on Internet service providers and law
20 enforcement in national security.

21 That sets out the sort of legislative basis, and
22 actually has an obligation. If you happen to look at
23 the first page on ISPs, to actually give officers and
24 authorities of the commonwealth assistance in relation
25 to enforcement of criminal laws, laws imposing pecuniary

1 penalties, protecting public revenue and safeguarding
2 national security, and to do their best to prevent their
3 networks and facilities being used against the
4 commission of offenses against the commonwealth and the
5 states and territories in Australia.

6 A couple of other interesting aspects of that,
7 because I think somebody in this panel or the last panel
8 was also concerned about the risks of being sued for
9 inappropriate disclosure. And under section 313 of the
10 Telecommunications Act of Australia, it provides that a
11 carrier is not liable for damages for an act done or
12 omitted in good faith to give reasonably necessary
13 assistance to officers or authorities of the
14 commonwealth states and territories.

15 So, there's an expression provision that
16 absolves the ISP from liability for the things done in
17 good faith to assist law enforcement agencies. But
18 that's the statutory context. And what Hugh's question
19 was really directed to was the voluntary process beyond
20 that, and in Australia, we have the Internet industry,
21 which has got together with a number of law enforcement
22 agencies to create what's now known as the Internet
23 Industry and Law Enforcement Agencies Cyber Crime Code
24 of Practice.

25 It's available for those of you that want to

1 have a look at this, in terms of the details of it, at
2 www.iaa, the Internet Industry Association, so
3 iia.net.au. The code recognizes a common interest
4 between the industry and government in prevention,
5 detection and investigation of online fraud to foster
6 user confidence. It confines itself to the cooperation
7 between ISPs and law enforcement agencies, but does
8 allow for future extension to hosting and e-commerce.

9 Under the code, ISPs are required to keep, this
10 is a voluntary code, not a mandatory code, but a
11 voluntary code, and under that code, ISPs are required
12 to keep the name, address, phone numbers, credit card
13 details and billing info of customers personal data, for
14 at least six months after a person ceases being a
15 customer, and dynamic IP allocation records and customer
16 log-out times and dates, what they refer to as
17 operational data, for at least one year after the date
18 of creation of the data.

19 Now, that code, it remains to be seen how
20 workable it is and how it's used in the future, but one
21 aspect of it that does potentially cause some problems
22 is the concept of interception. ISPs, many of the law
23 enforcement agencies don't have interception warrant
24 powers. There's no ability, for example, for the ACCC
25 in Australia to be able to get a warrant to intercept

1 telecommunications services or Internet services.

2 Interception in Australia has caused a little
3 bit of a problem, because recent legislative amendments
4 to obtaining information were proposed as part of the
5 anti-terrorism practice by the Australian Attorney
6 General's Office, and those amendments sought to
7 redefine, to an extent, when an email had been received.

8 So, when is something actually received, as
9 meaning when the addressee opened it on their PC, rather
10 than when it was received by the sender's server or the
11 service provider or other intermediaries, or the
12 recipient's service provider or the recipient's server
13 or the recipient's PC. It was being redefined to when
14 the recipient actually opened the email.

15 Now, although there were differing opinions in
16 Australia about the effect of that, there was a real
17 concern by law enforcement agencies that it had the
18 potential to stop them from obtaining any unopened
19 emails from suspect PCs without a specific type of
20 telecommunications interception warrant, like a wire tap
21 provision.

22 And the ACCC and other agencies, as I say, do
23 not have that ability, due to the concerns that we have
24 raised, that aspect of the package, the anti-terrorism
25 package, has been shelved, and it's been ordered to have

1 a further review in terms of our interception act
2 provisions. But they're the sort of technical issues
3 that are going to arise in some of this sort of
4 information in terms of interception, but I think that
5 code certainly does have the potential to provide a
6 global sort of informal process, voluntary process, but
7 I would be very interested to hear from some of the
8 firms here as to whether it's sort of achievable in the
9 volumes that we're dealing with that we were hearing
10 about earlier. Those sort of time frames, whether
11 they're realistic or not.

12 MR. BAMFORD: Just a few words following up on
13 that in terms of mandatory retention periods. In the
14 UK, we've recently introduced an antiterrorism crime and
15 security act. One of the elements in that deals with
16 the retention of communications data which will cover
17 traffic through an ISP, and the mechanism there is to
18 put in place some requirements to retain data for longer
19 than would be necessary for the ordinary business
20 purposes of the communications services provider in
21 question.

22 To say from a data protection point of view, our
23 laws, which I touched on earlier, do require that
24 personal data is held no longer than necessary for
25 the purpose, and if your purpose is various

1 communications over the Internet, so your business
2 purpose then is the retention period that's set. This
3 is a way of preserving it for longer.

4 In the UK when these provisions went into
5 Parliament as a bill and the provisions to retain the
6 data was expressed in ways that it could be retained for
7 a period of time for any criminal matter, but actually
8 as a result of scrutiny going through Parliament and
9 general concern, that actually changed to say that the
10 data that's retained can only be used for national
11 security purposes, i.e. to deal with things that do
12 touch on terrorism and not things that might be of a
13 serious nature in other ways, but not actually of that
14 serious nature, and we have a strange concept of a code
15 of practices part of this as well, but it shows that we
16 adopt a much more measured approach to the idea of
17 retention of that sort of data linked to a real pressing
18 need and harm, which in that case is terrorism.

19 MR. STEVENSON: I take it there you're focusing
20 on the provisions that are more system-wide as opposed
21 to the scenario, for example, that Eric proposed of it
22 given that you have a given case and a given
23 investigation and preserving information in relation to
24 that given matter.

25 MR. BAMFORD: Well, there's no actual mechanism

1 for any preservation as such in the UK context. In some
2 ways, that would be more privacy friendly. The general
3 retention of records for a period of, say, up to a year
4 with respect to any pressing need, so in some ways,
5 preservation of an actual problem is a better solution
6 in privacy terms than one which is a blanket retention
7 of data of all of a particular period in time. We don't
8 really have that provision.

9 MR. STEVENSON: Would you agree with that,
10 Cedric?

11 MR. LAURANT: Actually let me quote a recent
12 report that was released about one month ago, I think,
13 by a British Parliamentary company. This report shows
14 that a one-year data retention scheme if implemented
15 would be impractical, the costs have been
16 underestimated, and the Internet service provider and
17 the data communications industry have had so far few
18 incentives to implement any technical changes, not to
19 mention the fact, also, that the retention scheme
20 appears to be in breach of the United Kingdom human
21 rights legislation, which implements the European
22 Convention on Human Rights.

23 MR. STEVENSON: Thank you.

24 The other issue I would like to turn to,
25 quickly, and then if there's some questions I would like

1 to take those, is the scenario of suppose we've done the
2 investigation that Eric was able to get the information,
3 and the commission has pursued an action, then what
4 happens then?

5 MR. WENGER: Well, what happens then is we
6 typically will, for instance, if we're dealing with
7 somebody who we don't think will respect an order that
8 we serve upon them to stop, we will get a court order
9 that we serve upon registrars or web hosting companies
10 asking them to take down the content that we feel is
11 violative of the Federal Trade Commission Act.

12 And we've had, especially in the international
13 context, difficulty in doing that. And so I wanted to
14 raise for you that issue about whether or not you would
15 respect orders that are coming from foreign courts, are
16 there voluntary mechanisms for notifying you about fraud
17 that you would respond to, those sorts of questions.

18 MR. STEVENSON: Maybe if I could ask Chris and
19 then Kristen, do you have any response on that?

20 MR. BUBB: Well, we've had a lot of requests in
21 dealing with requests for taking down information on the
22 basis of violations of our terms of service. If you
23 come to us with an order that reflects a behavior that
24 is violative of our terms of service, we'll take them --
25 we'll take them off the service, and that has as much to

1 do with the fact that I think our terms of service are
2 at least as restrictive and I guess the short version is
3 we don't want this stuff on our service.

4 If somebody is being defrauded or somebody is
5 being injured in some way or if somebody is using a name
6 that is deceptive or using a practice that is deceptive,
7 we don't want them on our service. We're not a big web
8 hosting service, but if they certainly impact AOL we'll
9 take them down. And it's not so much in terms of the
10 fine points of jurisdiction or sovereignty, it has more
11 to do with the fact that we look at it on our service,
12 we don't want it there. So, it's consistent with that.

13 MS. VERDERAME: Yeah, I would agree with that.
14 We have pretty much the same procedure. And building on
15 a point that was made earlier with regard to consent,
16 that is one of the exceptions for data protection rules.
17 So, we have, in fact, built into all of our contracts in
18 contract hosting limitations on use. If we find out
19 that a user or customer is using web hosting services in
20 any way that is fraudulent or unlawful, we word that
21 extremely broadly on purpose, we have the right to
22 immediately terminate the service, and we, in fact, do
23 that, if we receive a request or a complaint that's
24 substantiated.

25 We also build it into contracts that we have

1 with our ISP business. We notify customers in our
2 privacy policies all over the company, whether it's
3 retail customers, whether it's content hosting, whether
4 it's business service customers, we specifically say in
5 our privacy policy, if you break the law, if you use our
6 services to break the law or do anything fraudulent, we
7 will give your information over to law enforcement if
8 it's legitimately requested.

9 So, we do install that into our practices and
10 procedures based in part on the data protection regime
11 that we have to work with. But I think it's the same
12 procedure that AOL follows as well.

13 MR. STEVENSON: Thank you. We have time for a
14 couple of questions, if there are some. If people have
15 questions or comments that they want to address to the
16 panel. We have one here.

17 MS. KLEIMAN: Kathryn Kleiman for the
18 Association of Computing Machinery's Internet Governance
19 Project. A question for Mr. Bhojani, I hope I
20 pronounced that correctly. The law that you cited in
21 Australia, that enables cooperation between say the ISPs
22 and registrars and law enforcement. What does that do
23 in the situation where ISPs and registrars are contacted
24 directly by foreign law enforcement? Let me give you
25 two scenarios, please.

1 One scenario would be being contacted by the
2 Federal Trade Commission of the United States, regarding
3 a fraud investigation. Are the registrars and ISPs free
4 to cooperate and are they free of liability if they do?

5 The second question is what if they're contacted
6 by the Chinese government regarding a domain name that's
7 being used for pro democracy, anti-Chinese information?
8 Same thing, do they hand the information over? Do they
9 notify the registrant? Do they cooperate? Are they
10 free of liability, if they do?

11 MR. BHOJANI: Thank you. Unfortunately, the
12 laws that we're talking about really are focused on laws
13 of the commonwealth of Australia. So, really it's
14 protecting the ISPs insofar as they're assisting law
15 enforcement agencies at a domestic level, rather than on
16 the international level.

17 It would still be a requirement, I suspect, in
18 terms of the dialogue we've been having here, that most
19 of the ISPs would want to see a court order before they
20 would touch anything in an international context.

21 MS. KLEIMAN: An Australian court order?

22 MR. BHOJANI: Well, a foreign court order that
23 they would be willing to recognize that they are somehow
24 absolved of liability. The liability provision that I
25 was referring to was, again, protecting them from

1 liability where they act in good faith to assist
2 Australian law enforcement agencies, rather than
3 international law enforcement agencies.

4 The point that Kristen made and others have made
5 as well, the ability to work through local agencies in
6 that context, it might be that the FTC would come to the
7 ACCC to try to get assistance from us, or the Chinese
8 government would do likewise. And we might be able to
9 see whether there's something that breaches our law that
10 we might be able to go to the ISP with as well. And
11 that combined might be able to achieve an outcome that a
12 direct approach may not be able to achieve.

13 MS. DEUTSCH: Kathy, I just wanted to give you a
14 real example from Australia that I just read about two
15 days ago. The members of the recording industry have
16 demanded from the universities, who are also ISPs, that
17 they turn over essentially all of their traffic data on
18 their networks to the recording industry companies so
19 that they can scan this information for their own
20 purposes.

21 MS. KLEIMAN: Has there been any response?

22 MS. DEUTSCH: I think that the universities have
23 the data but they haven't yet said what they are going
24 to do.

25 MR. STEVENSON: Alistair, did you have a

1 question?

2 MR. TEMPEST: Thank you very much. Excuse me,
3 because I missed yesterday for various snowy reasons,
4 and it may well have come up yesterday, but I thought it
5 was a point which has been raised just now and which
6 Sarah raised right at the beginning of this panel, which
7 I think is very important. That is, the application of
8 national laws as compared to the application of actions
9 against criminals. I think there is actually a very big
10 difference.

11 When, for example, someone breaks a law which
12 creates fraud, that is something which I think nearly
13 everyone can accept across the world. Because there is
14 a damage to an individual or whatever it happens to be.
15 The issues that we start to look into here, particularly
16 on things like data protection or the issue which was
17 just raised where someone has broken the law in China,
18 and someone is being asked in Australia to apply that
19 Chinese law is something a lot different and creates a
20 major problem.

21 There is, of course, the Hague Convention which
22 is going on at the moment. In Europe we have an issue,
23 and a very live debate about three conventions on
24 jurisdiction, and where that jurisdiction should be
25 applied, should it be applied in the country of

1 destination, or the country of origin. And I think that
2 is an area which, perhaps, there will not be such an
3 easy international agreement as some of the other
4 discussions we've had today, but I don't know what the
5 other panelists feel.

6 MR. BAMFORD: It's partially touching on the
7 point that you raise in there, Alistair, which I mean,
8 some of those are bigger issues than anyone in this room
9 can decide, I suspect. But if we come down to sort of
10 practicality in terms of the information and sharing end
11 of things and the information disclosure end of things,
12 I think when you're actually talking about what's the
13 appropriate data to share, you know, we do need to
14 manifest this in some sort of memorandum of
15 understanding, information sharing protocol between
16 appropriate agencies to give people confidence that
17 actually the information that's being shared is for
18 things which would be legitimate concerns in both
19 countries in terms of it being related to the loss and
20 not the Chinese example or Iraqi example or anything
21 else you might want to bring forward which might not be
22 absolutely coterminous with an offense in any of our
23 particular countries, but I think as well it's an
24 opportunity, and I think Cedric was touching on this as
25 well, to put in place something which sets the

1 boundaries then in terms of what can happen with the
2 information.

3 Because I know from a data protection point of
4 view, one of the things that does worry us is that when
5 somebody provides information initially for bona fide
6 reasons, once that's gone to somebody else, what's the
7 ring fence that's being applied on it being used in any
8 other ways? And we've had this with disclosures to U.S.
9 authorities in the past, well, I shouldn't say European
10 police office, Europol, for terrorism. When we looked
11 at essentially the number of people who could have
12 access to this, it was 20 some thousand U.S. enforcement
13 authorities.

14 We sort of a differ a little bit at that point
15 from a European perspective, there is a very, very wide
16 disclosure that's going to take place, information
17 sharing agreements, protocols, perhaps can start to set
18 some of the boundaries of reassurance there, how long
19 the data is held for, those sorts of reassuring points
20 there, and indeed mechanisms, and this came up
21 yesterday, to make sure that if the data changes and the
22 finger of suspicion has been lifted from somebody, then
23 that information gets passed on as well to make sure
24 that records are kept up to date.

25 And we have plenty of experience in the UK of

1 multi-agency approaches to information sharing where
2 people don't really deal with it in a very professional
3 way and there's all sorts of impacts on people's private
4 lives as a result of that. I would worry about that in
5 the international context.

6 MR. STEVENSON: Any other questions? Eric?

7 MR. WENGER: Two things I wanted to point out.
8 With reference to the point that Cedric made about the
9 need for information, I think it's an excellent point.
10 And I think at the FTC we're especially cognizant of the
11 balance between privacy and law enforcement. And the
12 scenario that I posed was actually assuming that we
13 found something that was fraudulent that we believed
14 needed to be investigated, but I think particularly here
15 where we are a regulator that enforces laws that relate
16 to privacy and also have worked hard to promote privacy
17 in the private industry, that that is a point that we're
18 very aware of and cognizant of.

19 Also, I think we're also very cognizant of the
20 costs that are associated with preserving data for
21 open-ended periods of time. And so we do understand
22 those concerns. And finally, I wanted to take up the
23 challenge that was raised by Commissioner Swindle in the
24 first place about talking about the good as well as the
25 bad.

1 And I think that I wanted to make sure that
2 everybody understands that we actually have had very
3 positive experiences dealing with Internet companies
4 that have set up special contacts for us when we're
5 conducting investigations that we can reach out to, that
6 have allowed us to use fax or email ways to communicate
7 with them to speed up the time frames and get
8 information back in response to our subpoenas quickly,
9 and who have preserved data upon request and in response
10 to our subpoenas, turned that data over to us in timely
11 ways. And the ability for us to get that information
12 has been vital to our success in fighting Internet
13 fraud.

14 MR. STEVENSON: Thank you. Eric, and I wanted
15 to adjust one point in response to the issue that
16 Alistair raised about the jurisdiction and conflicts of
17 law. I think there are obviously very great
18 difficulties that go on in a lot of those issues, and it
19 is a challenge, and I think one of the reasons that we
20 in the OECD, Commissioner Thompson is describing, our
21 joint work there on cooperation to address cross-border
22 fraud and deception, and one of the challenges there is
23 we were picking an area where, as Alistair suggested,
24 there is some common understanding of an area where the
25 conduct is problematic, no matter where it's occurring,

1 and frankly even then, we have a lot of challenges as we
2 hear and how do we best cooperate, but the idea is to
3 focus on precisely that kind of conduct and develop
4 these connections so that we can make progress forward.

5 We have run out of time, and the press
6 conference will be here in just a few minutes, then we
7 will start back up at 2:15 sharp with our panel on
8 domain name registrars, so I will end by thanking our
9 panelists for what I thought was an excellent
10 discussion. Thank you very much.

11 (Applause.)

12 (Whereupon, at 12:45 p.m., a lunch recess was
13 taken.)

14

15

16

17

18

19

20

21

22

23

24

25

1 AFTERNOON SESSION

2 (2:15 p.m.)

3 MS. MITHAL: Okay, why don't we get started.

4 My name is Maneesha Mithal and I am the
5 Assistant Director for International Consumer Protection
6 here at the Federal Trade Commission and I would like to
7 welcome all of you to this panel on cooperation between
8 consumer protection enforcement agencies and domain
9 registrars and registries.

10 As you can see, we have a very large panel
11 today, and it's actually a fairly long panel and we're
12 hoping to cover many issues, but I thought it might be
13 useful to start by just setting some ground rules so
14 that we can streamline the discussion.

15 The format of this will be moderated discussion,
16 so I will just throw out issues and questions. When you
17 would like to respond or if you would like to respond to
18 another panelist, just please raise your tent and wait
19 to be called on by me. This part is very important, I
20 would just ask that all of the panelists keep their
21 remarks as short and succinct as possible, and as to the
22 point as possible.

23 I promise you that if we all adhere to that
24 rule, everyone will have multiple opportunities to
25 speak. And I just want to give you fair warning that,

1 you know, we do have a lot of issues to cover, and
2 please don't be offended if I ask you to move along or
3 finish your points.

4 So, to that end, I thought it would also be
5 helpful if we divided up the panel into segments. I
6 thought we would spend the first half hour or so talking
7 about whois data in the generic, top-level domains. I
8 thought we would spend the second half hour or so
9 talking about whois data in the counsel domains, and
10 then we can take a short break and talk about
11 information sharing generally between consumer
12 protection enforcement agencies and domain registrars
13 and registries.

14 And then finally spending about a half hour or
15 so talking about how we can suspend fraudulent websites
16 and how we can work together on that. And this panel
17 should wrap up right around 4:30 or so and we should
18 have an opportunity for people from the audience to ask
19 questions.

20 So, let me also just start by defining some
21 terms here. I think most of you are familiar with them,
22 but for the benefit of those of you who haven't, we'll
23 be using the term "whois" a lot. Whois refers to a set
24 of databases where domain registrants' contact
25 information can be found.

1 We'll be saying the word GTLDs quite a bit.
2 GTLDs refers to generic top level domains, those are
3 domain names ending in .com, .org, .net, .info, .bus and
4 some others. And those domains are generally regulated
5 under contracts ICANN or the Internet Contact for
6 Assigned Names and Numbers.

7 And then we'll be talking to you about CCTLDs
8 quite a bit and those are country code top-level domains
9 and those are domain names ending in two letter country
10 codes, like .UK or .GE for Germany.

11 So, with that, why don't we jump right into it.
12 I thought it might be useful to set the stage a little
13 bit, and so I want to ask Dan Salsburg from the FTC to
14 talk a little bit about how we use the whois database in
15 our investigations.

16 MR. SALSBURG: The whois database or databases
17 really are the first steps we take in most of our
18 Internet fraud investigations using these databases. We
19 routinely go to the databases to find out who is
20 responsible for the given website, the name of the
21 registrant. We try to find out from whois databases the
22 identity of the registrar who can be served with process
23 and we can make requests upon for additional
24 information.

25 We look at the address information that shows up

1 in whois listings to determine where is this business
2 located. We look at the host information to find out
3 where the servers are located. In short, without whois,
4 we have a very difficult time finding out who has
5 responsibility for a website that may have some
6 fraudulent claims on it.

7 We also use the whois database in another area,
8 and that is oftentimes, in addition to the work we do
9 stopping frauds, we engage in what are called surf days,
10 which are designed to identify the prevalence of fraud
11 or activities that appear that they may have fraudulent
12 components, and inform the purveyors of those websites
13 of the problems with their websites and ask them to
14 respond.

15 For instance, often we will get together with
16 state attorneys general or with our counterpart consumer
17 protection agencies with other countries and we will
18 review numerous websites, if we find problems with
19 websites we will send emails to the people or the email
20 addresses that show up in the whois database under the
21 contact information and try to inform them of the
22 problems that we saw with the website.

23 MS. MITHAL: Dan, can I just follow up. Could
24 you lay out some of the -- do we face any concerns with
25 the whois database right now?

1 MR. SALSBURG: Yeah, there are a number of
2 problems, but the two principal ones are first of all
3 the accuracy of the data in the whois database. We have
4 seen in one case we had there was a registrant that was
5 engaged in some pornographic commerce, and it happened
6 to be listed in his whois entry as being located on
7 Foreskin Street in Amsterdam with Amanda Huginkiss as
8 the administrative contact. Clearly we had a difficult
9 time figuring out who was responsible for that website
10 based on the whois data.

11 In a similar instance, there was a case that
12 didn't have as interesting a false entry, but there was
13 a case we had where the address was Herehere,
14 California. We have also found websites registered to
15 Mickey Mouse, to God, to Hacker, Bill Clinton, FBI, you
16 name it. And the inaccurate information is really a
17 serious problem.

18 The second major problem that we have with the
19 database is the searchability. We can go back a few
20 years ago, and the .com registry, there was only
21 Verisign, or Network Solutions at the time, that was the
22 sole registrar for .coms. And at that time, when it was
23 all centralized, it was much easier to conduct our
24 investigations.

25 With the advent of competition amongst

1 registrars, what we have found is we are having a more
2 difficult time in finding out additional information
3 about websites through usage of the whois database. And
4 principally, up until about a year ago, you can go to
5 the Verisign whois database and you could search on
6 multiple fields.

7 So, you could search under the name of a
8 registrant and you could find out a listing of
9 several -- there was a time-out on it, but substantially
10 all the websites registered to a given person. Which
11 helped us considerably, because what we find in case
12 after case after case is the perpetrators of a fraud
13 often have multiple websites that they use, and if we
14 can't search across multiple fields, such as an address
15 field or a name field for the registrant, we are only
16 going to see one part of a fraud and we are going to
17 miss all of the other tentacles that emanate from it.

18 MS. MITHAL: Thanks, Dan. Dan, you mentioned
19 two issues, the first is I guess accuracy and the second
20 is searchability and I thought we could use that as a
21 framework in our discussions for this issue.

22 So, first about accuracy, I know that the OECD
23 has done some work on this topic and I thought I would
24 ask Michael Donohue to describe some of that for us.

25 MR. DONOHUE: Thank you, Maneesha.

1 I would like to be able to talk about the kind
2 of work that we have done at the OECD, but it's really
3 work worth doing and we haven't quite finished it, so I
4 can't say where exactly it will end up, but it's been
5 going on for some time. It involves primarily the
6 consumer policy committee at the moment, but tax revenue
7 experts as well have been looking at the issue, and even
8 going further back, some of the Telecom policy folks.
9 We also have privacy and security experts, so we're
10 trying to all talk to each other to come up with some
11 common themes.

12 In the consumer area, we're looking at it from
13 the perspective, two perspectives, really, one is with a
14 view towards increasing transparency integrity of domain
15 names for consumers themselves, and this comes out of
16 the OECD guidelines, the 1999 guidelines on consumer
17 protection in the electronic commerce, which called for
18 businesses to identify themselves for the benefit of
19 building consumer trust.

20 The other primary and really in a sense more
21 critical uses for that are consumer protection law
22 enforcement, working so that Dan and his counterparts
23 around the OECD countries can do a good job protecting
24 consumers by identifying websites that are committing
25 fraud.

1 And, again, this is work that flows out of the
2 guidelines to some degree, again, one principle calls
3 for businesses to identify themselves, not just for
4 consumers, but also for law enforcement. The focus here
5 is on commercial usage of the Internet, of course.

6 MS. MITHAL: I'm just curious, does anybody have
7 any statistics on accuracy of whois data, anything that
8 people know about the ICANN complaint form where people
9 can file complaints about accuracy?

10 Mike?

11 MR. PALAGE: I was talking to Dan Halloran, and
12 I believe that the Internet GOTNET website has been up
13 now for about six months, I believe, and I believe that
14 they have received approximately 4,500 complaints to
15 date. Now that would just be in the .com, .organize and
16 .net space. The most interesting statistic that Dan has
17 relayed to me has been in connection with most of the
18 complaints are related to spam.

19 So, the majority of the complaints, people
20 submitting, if they do state a reason why they believe
21 it's inaccurate, has generally been in connection with
22 spam that they've received.

23 MS. CADE: If I can just add to that.

24 MS. MITHAL: Would you identify yourself.

25 MS. CADE: I'm Marilyn Cade with AT&T and I am

1 the cochair of the Whois Task Force. Just to follow on
2 what Michael said, they actually today have received
3 over 6,000 complaints. So, the number of complaints and
4 the usage of the centralized form is really working
5 quite well, and there's been apparently significant
6 increase using the complaints as people have become
7 aware of the availability of the Internet form.

8 MS. MITHAL: Dan?

9 MR. SALSBURG: Sure. We recently engaged in a
10 search with fellow law enforcement of based on spam that
11 had remove me or unsubscribe lines, and then we went to
12 the whois databases and we got the email addresses for
13 the websites and sent out emails asking to be
14 unsubscribed or removed, and I believe 21 percent of
15 those email addresses that appeared in the whois
16 database were false, they were inaccurate.

17 So, I imagine it's impossible to extrapolate
18 from that that 21 percent of all entries in the whois
19 database are inaccurate, but certainly in websites that
20 have claims that appear to be deceptive, inaccuracy is a
21 serious problem, and those are the types of websites
22 that we really care about.

23 MS. MITHAL: Marilyn, I know you mentioned you
24 cochair the Whois Task Force and I was wondering if you
25 could summarize some of the recommendations of that task

1 force with respect to accuracy of whois data.

2 MS. CADE: Sure. I would love to do that,
3 particularly since some of the other panelists here
4 either helped to launch the task force, Paul Kane, or
5 are on it now, Phillip Grabansee, we've all worked very
6 hard to try to reach a set of recommendations. When the
7 task force began with a survey and some of the findings
8 of the survey, I will just very quickly mention, because
9 I think they may be of relevance to this.

10 We did ask people in the survey how they use the
11 whois database, and the uses of the database are the
12 kinds of things that one would expect, people use them
13 in order to find out who is behind or operating a
14 website. They use it in order to solve technical
15 problems, they use it in order to find out whether or
16 not a domain name is available to register, and of
17 course law enforcement uses it. Sort of the typical
18 things that one expects.

19 But the things that might be kind of
20 interesting. We asked the question of what best
21 describes your attitude toward access to the data in the
22 whois service, and the findings are as follows: And,
23 again, this is a survey that was done more than a year
24 ago, we don't consider it statistically valid, but think
25 of it as a snapshot of what people have responded from

1 their own personal views.

2 Forty-two percent use whois as effective
3 identification of who is behind a specific domain for
4 consumer protection or intellectual property protection
5 purposes. Another 27 percent think that it should be
6 available and accessible because it supports the
7 resolution of technical problems on the Internet. And
8 another important point that is important to make is
9 that 20 percent of the respondents did identify an
10 interest in protecting the privacy of individual domain
11 named holders.

12 So, when people responded to how they used it
13 and what they thought about access, the primary
14 responses were in those three areas. We found that 42
15 percent of the respondents said they had been harmed or
16 inconvenienced, and that of that, close to 40 percent
17 said that the data of the whois records they relied on
18 were inaccurate, incomplete or out of date. So, roughly
19 40 percent said that the whois records that they're
20 accessing, not all just because of fraud, were
21 inaccurate or out of date.

22 The task force has recommended an initial short
23 set of recommendations. Data is not always inaccurate
24 on purpose. We tend to think as law enforcement or as
25 companies who are dealing with enforcement

1 responsibilities, which we may have in dealing with
2 fraud, we're mostly looking at the data that is someone
3 who may have purposely put in wrong data, but a lot of
4 the data is aged, and so you can't be contacted because
5 your contact information is just too old, it's gone old.

6 So, one of the recommendations is that once a
7 year, the registrars contact the registrant, present
8 their registration information details to them, and ask
9 them to correct it. And then it is the responsibility
10 of the registrant to do that.

11 The other recommendation that we made in the
12 area of accuracy is that we provide that I can provide a
13 what we would call a safe harbor. If someone has lost
14 their name, because of providing inaccurate data, that
15 they would go into a redemption grace period of 30 days,
16 and if during that period they presented correct contact
17 information, they would be able to recover the name.
18 It's out of the zone, but they haven't lost it.

19 The second area of recommendations address the
20 use of bulk access of the whois data, and the task force
21 broadly, and supported by the community, expressed
22 strong concern about marketing uses of whois data. The
23 survey itself expressed strong concern about marketing
24 uses of whois data. Think of it as using the data for a
25 purpose other than that for which it is collected. I

1 suspect that's a phrase that rings to some of my
2 colleagues's ears, and that was strongly supported by
3 the task force.

4 So, our first recommendation was to limit all
5 marketing uses of bulk access to the data. Those are
6 the primary consensus policy recommendations. We've
7 made other recommendations that I can maintain the
8 centralized report process for reporting, other things
9 of that nature.

10 MS. MITHAL: Well, why don't we just focus on
11 the accuracy part of the report and I want to
12 throw open the floor and see if anybody has anything to
13 add or if anybody has any concerns about the task force
14 report.

15 Ruchika Agrawal?

16 MS. AGRAWAL: Part of the Whois Task Force's
17 report is to report accuracy, and to me that's like
18 putting the cart before the horse, because surveys have
19 consistently showed that one of the reasons users
20 provide inaccurate information is because there are no
21 privacy safeguards in place.

22 So, one way to improve accuracy within the
23 question that you've posed, Maneesha, I think is to
24 provide and implement privacy standards.

25 MS. MITHAL: I saw Phillip first and then

1 Henning and then Kathryn.

2 MR. GRABANSEE: A concern with the report, which
3 was participated by myself on the task force, but just a
4 point that I would like to add from a registrar point of
5 view, just something, I don't have a solution to that
6 problem, but just something to keep in mind. It's an
7 economic problem for the registrars, you know, they are
8 operating in an environment with selling domain names
9 with very small margins, and the more burden you put on
10 the registrars, checking the accuracy of whois
11 information, which we all want to be accurate, of
12 course, but it makes it more difficult for the
13 registrars who are already operating in such a difficult
14 economic environment, and it might lead, you know, I'm
15 not sure, but it might lead to a point where we have
16 only, you know, very few registrars who can survive in
17 that environment, and that's something that was
18 certainly not desired when the whole Internet and the
19 whole domain market was demonopolized.

20 So, I just want everyone to keep in mind that
21 the more burden you take to the registrars, which of
22 course is necessary, because they have to participate,
23 but it has strong economic implications, especially for
24 the smaller and medium-sized registrars and will change
25 the market as we see it right now.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

1 MS. MITHAL: Actually, just before we go to the
2 next comment, I think those two comments provide a good
3 framework for discussion, and I would urge other people
4 to comment on those two comments. Ruchika raised the
5 concern of privacy concerns and putting the cart before
6 the horse and that the privacy concern should be
7 addressed first and then Phillip raised the point about
8 costs imposed on registrars. So, in particular, I would
9 like to hear from people about those two points and what
10 they think of those.

11 MR. GROTE: My name is Henning Grote, I am with
12 Deutsche Telecom of Germany. Just adding to Marilyn's
13 data from the whois report, we found that due to the
14 fact that most of our DNS customers, our registrar
15 customers, are business users, I would say the aging of
16 the data is about relevant for 20 to 30 percent of the
17 data of the whois per year. This is the kind of rate
18 that gives you an approximate idea of the aging of the
19 data.

20 The other thing, adding to that what Phillip
21 just pointed out, indeed, it's a big problem to have the
22 costs within a framework that's somehow -- makes it
23 somehow possible to handle in the economic model. But
24 on the other hand, on another technical field, we just
25 started the ENUM trial in Germany, the electronic number

1 mapping trial where the telephone numbering system is
2 mapped on the -- on a DNS basis.

3 So, within this trial, for example, we have
4 installed the -- as mandatory -- the policy to validate
5 and verify the registrant. Validate the number that is
6 sent in that should be transferred onto the email name,
7 and verify the registrant, the person, the individual
8 who is seeking after having this number registered.

9 So, we have now the challenge to put those two
10 worlds together, because one thing is sure, when ENUM
11 indeed goes into reality, and indeed becomes a stand-out
12 technology, we do have to handle this issue of
13 verification and validation of data, at least in Germany
14 as opposed to in most other countries using ENUM, there
15 will be a similar policy.

16 On the other hand, the issue of costs and the
17 very small margin product DNS. So, this is quite a
18 challenge.

19 MS. MITHAL: Actually, let me just ask a
20 follow-up question to both Henning and Phillip. You
21 both mentioned the cost issues. Do you have concerns
22 about the costs that the specific recommendations of the
23 Whois Task Force report would impose on registrars?

24 MR. GRABANSEE: It will certainly be a concern
25 and problem for the -- it will certainly raise some

1 problems for the registrars. I mean, if you believe in
2 a free market model, you can always argue easily, okay,
3 finally the market has to show that the prices for
4 domain names, I mean the prices registrars take for
5 domain names, they are not regulated.

6 So, I mean, registrars theoretically are always
7 free, if they can make it or produce it or cannot show a
8 business model to increase the prices, but this will
9 take a long time and this whole procedure will probably
10 put a lot of smaller registrars out of business. And
11 the question is if that is desired, or the other
12 question, you can say that free market interest is just
13 like it is, but I don't have a clear answer to that
14 question. I just see the problem.

15 MR. GROTE: Just to follow up on that. The
16 question I'm just asking myself is whether the small
17 margin, very low quality product DNS, in some cases,
18 will have a future under these circumstances. The
19 question might be whether other business models should
20 arise, or might arise. Well, I don't have an answer to
21 Phillip's concerns, neither do I have an answer to my
22 own concerns, when it comes to elaborating on a new
23 business model.

24 I don't know a lot about that, but one thing is
25 for sure, when the -- let's say the quality aspects of

1 the DNS services, like a curacy, and let's say like a
2 data handling where the customers can rely on, when
3 these are aspects that count, that also means that
4 the -- that our customers have to be educated.

5 That's on our side. And that's quite an issue.
6 It still has lots of costs, but I would like also to ask
7 the question when we don't do that, how might the market
8 go, and into what direction? Would it go totally down
9 because of the total distrust on the consumer side? I
10 don't know. Just a question. Just a thought.

11 MS. MITHAL: Okay, Kathryn?

12 MS. KLEIMAN: I wanted to shed a little light on
13 the privacy issue. And just for whoever hasn't used the
14 whois database, it's a globally available database.
15 When you go to it and you put in information, you get it
16 with the click of a button. For those of us who
17 register domain names for our personal hobbies, to
18 express personal concerns that we have, say, racism or
19 antisemitism, to criticize large corporations for
20 adopting intellectual property policies that we think
21 are too broad, or for political speech, such as human
22 rights or corruption in countries, we don't want our
23 telephone numbers and home addresses available at the
24 click of a button.

25 The first question that we were asked in

1 preparation for the panel was how can domain registrars
2 and registries improve the accuracy of whois data and
3 the generic top level domains? There's one easy answer,
4 and that's called tiered access, effectively create the
5 option of an unlisted telephone number or home address.

6 I come from a technical organization, the
7 Association for Computing Machinery, we've been around
8 since 1947, many of our members were original Internet
9 pioneers. When you go back to them and you ask them
10 what the purpose of the whois data was, they said it was
11 for technical contact. It's to reach someone if your
12 website was sending out, you know, unheard of amounts of
13 crap on the 'net and you needed to shut it down. It
14 wasn't for the purpose which it's increasingly being
15 used for, which is content policing.

16 So, of course law enforcement needs to reach
17 people, as do others who are suing based on content, but
18 the whois database as it exists is inaccurate because
19 people are trying to protect themselves. Very much in
20 the way, frankly, that the Federal Trade Commission has
21 advised people to do in their consumer identity theft
22 publications, where they say, don't give out personal
23 information on the 'net. That's very good advice.
24 Don't give it out.

25 So, my best recommendation as we go into this

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

1 is, let's draw a very clear distinction, and it hasn't
2 been drawn, in the Whois Task Force report, let's draw a
3 very clear distinction between commercial use of domain
4 names and noncommercial use of domain names.

5 The second thing I would raise as domain
6 registrars pose the issues of cost is the issue of
7 liability. This is not my organization, but it has been
8 xeroxed and distributed, the Electronic Privacy
9 Information Organization, bullet point number two,
10 yesterday, "The New Hampshire Supreme Court has held
11 that information brokers and private investigators can
12 be liable for the harms caused by selling personal
13 information. In that case, a young woman was murdered
14 by a stalker who obtained her personal information from
15 information brokers and private investigators."

16 To the registrars, I would say, we are your
17 subscribers. You know, there are people out there,
18 there are disgruntled spouses, there are stalkers, there
19 are governments who want to criticize people for taking
20 democratic, pro-democratic positions, protect your
21 subscribers. Let's figure out a balance, but the single
22 best answer to protecting accuracy, to getting accuracy
23 to whois is giving people the right to create an opt-out
24 where the information is there, it's available to law
25 enforcement and others under the appropriate

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

1 circumstances, but not to the whole world all at once.

2 MS. MITHAL: Before we move further, let me just
3 talk about some of the scope of the discussion we're
4 having here. I think the scope of this workshop is
5 about cooperation between law enforcement and domain
6 registrars and registries in combatting fraud, and I
7 think the points Kathy just made are extremely important
8 points, and I think, you know, those issues definitely
9 need to be discussed further, but I'm wondering for the
10 purposes of this discussion, if we could simply talk
11 about whois data for commercial registrations, the types
12 of investigations that we do generally involve
13 commercial targets.

14 So, if we just limit it to that for the purposes
15 of this discussion, as people are talking further, I
16 just ask you to do that.

17 So, Paul and then I saw Willie, and then Dan.

18 MR. KANE: Thank you, Maneesha.

19 My name is Paul Kane, ICB from the UK. We are a
20 software house, and we've built a number of systems for
21 quite a few registrars. Just to bring this to
22 perspective, there are 160 ICANN accredited registrars,
23 of which 118, I believe, are currently active. I think
24 it's fair to say that every registrar that is active
25 really would like to provide to the community accurate

1 information. They don't go out purposely to allow
2 Donald Duck, as the gentleman referred to.

3 One of the things, I think registrars will be
4 very concerned about, is where the duty of care to check
5 the accuracy actually rests. And that, as Kathy was
6 implying, has costs, and there are some significant
7 issues. And obviously at what point is the data
8 accurate?

9 At the time of registration, the applicant may
10 have submitted accurate information, and then the day
11 after registration, the person may have moved, there
12 could be a change in circumstance. So, if one
13 delineates between commercial registration and living,
14 breathing individuals, who may require a degree of
15 privacy, because it seems the privacy issue is the one
16 of concern, and in fact the lady at the end there
17 mentioned it, I think it's fair to say within the ICANN
18 accreditation agreement, that registrars sign in order
19 to be able to register in the gTLD lease space, there is
20 already provision for registrants to use the contact
21 information of a third party, where they feel that
22 personal freedom, personal liberties may be infringed.

23 And so, the mechanism already has that in place.
24 So, the registrar can accurately record the information
25 of a third party. Now, there may be a cost associated

1 with the provision of accurate information of a third
2 party, but obviously that is the choice of the
3 registrant in exercising that right, if they wish to do
4 so.

5 We have the pleasure of having Jonathan Bamford
6 here from the UK Information Commissioner's Office, and
7 obviously being from the UK, one of the things is
8 explicit consent, one has to give consent to information
9 being publicly disclosed. And similarly, provided that
10 information, the registrant at the time of registration
11 is aware the information will be publicly disclosed, I
12 think it's fair to say that the registrars will be
13 covered, provided it's made very clear to the registrant
14 at the time of registration it will be available on the
15 Worldwide Web.

16 And then Henning raised a pretty good point
17 about ENUM. My company, Nominet, are actually involved
18 in the UK in the trial, we're going to be running the
19 tier one where the .44 is going to reside. And one of
20 the big costs that the domain has in the ENUM is not
21 register the domain, it's matching a particular
22 telephone number with a subscriber with an entry.

23 And so, in the domain name market, which is
24 global by its very nature, one has to be very careful
25 insofar as the duty to supply the registration rests on

1 the registrant, not any other party. In the case of
2 ENUM, it is the person requiring a number that will need
3 to come with their telephone bill that identifies them,
4 the address, and the phone number. There will be a duty
5 on the registrant. Similarly, within current contracts,
6 I think it's fair to say that registrants place that
7 duty on -- sorry, registrars place the duty on their
8 registrants to provide accurate information.

9 And the whois report is really trying to make
10 sure that the information that is held on the central
11 database is accurate, subject to these conditions. It's
12 in the registrars' interest to make sure they're
13 accurate, because they want to be able to contact their
14 customers. As I say, there is already provisions to
15 protect living, breathing people.

16 Another angle, just to complicate matters, is in
17 Austria, the rules are such that companies, corporate
18 entities, not living, breathing individuals, corporate
19 entities can similarly claim a degree of protection
20 under data protection. So, it's very difficult to draw
21 a line because commercial entities and living, breathing
22 people. But it's not in the registrars' interest to
23 gather up bogus information.

24 MS. MITHAL: And just a follow-up question. You
25 mentioned that individuals have a protection that they

1 can register through a third party. If I'm a company
2 that's selling, you know, fraudulent goods to consumers,
3 could I hide behind that as well?

4 MR. KANE: The duty, again, is to the
5 registrant. There is a relationship, a legal
6 relationship between the third party agent and the
7 registrant. Assuming because the third party agent
8 would not want to be liable for any of its customers.
9 So, from a law enforcement perspective, it is quick and
10 easy to identify the third party, and having done so,
11 they can get a direct relationship to the registrant.

12 So, it's all there, it just needs to be applied.

13 MS. MITHAL: Willie?

14 MR. BLACK: Thanks. I'm Willie Black, chairman
15 of Nominet UK who manages about four million domains in
16 the .UK top level.

17 I'll try and be quite brief. I think I'm
18 complementing what other people say. It's important to
19 us to know who the other party to our contract of
20 registration is. After all, it is a contract, and you
21 don't want to contract with somebody that you can't
22 chase out for money. But it's very human intensive,
23 what we're talking about here.

24 In the UK, we have money laundering things, and
25 if you try and open a bank account, you've got to send

1 in a copy of a utility statement or a copy of your
2 passport or something like that, and this has to be
3 verified. It's very human intensive. And in Nominet,
4 we've just realized that we cannot keep affording to do
5 too much intensive human checking. Which is a pity
6 really, but if it has to be done, of course we will be
7 happy to try and do it as sufficiently as we can.

8 But even in spite of the cost, you see, good
9 people do want their data to be correct, and I'm here
10 talking about trading, not the personal one, and we do
11 give an opt-out in .UK to people to register an agent if
12 they want to hide, because of personal threats.

13 But talking about businesses, good people do
14 usually want their database to be correct, and so
15 they -- the whois is useful for them to check that it's
16 correct, but the lot of them are very lazy and they move
17 premises and they just forget to change things.

18 So, again, a renewal period of two years that we
19 do is actually quite a good time to be catching up with
20 people. Although you might just find that you send the
21 invoice out and you never get any money back. And then
22 there's a lot of problems.

23 But the real point of my intervention is, is the
24 crooks actually are quite clever. They don't go around
25 with a bag marked swag, you know, or a striped jumper,

1 and they're not going to write Mickey Mouse down when
2 they're perpetrating 100 million pounds in fraud, huh?
3 They're going to put a perfectly reasonable business
4 name that you just can't trace very easily.

5 And of course before there's an issue arises,
6 nobody can tell that it's wrong, without you going and
7 checking that such and such a street number at such and
8 such a place actually exists is going to look perfectly
9 reasonable. And so you can only react once it's been
10 discovered. And of course the registries would be very
11 happy to try and chase down the issue at that point and
12 see if there's any forensic evidence that it would be,
13 you know, that it was some real business or a fraudulent
14 business.

15 One thing that we do suffer from in the domain
16 name business is that we are private entities. We don't
17 have the power to fine. If you declare the wrong thing
18 on your vehicle license in the UK, I think it's a
19 thousand pounds, you can be fined. Because there are
20 statutory bodies and they can fine you for making a
21 misdeclaration. I don't know how often it happens in
22 the UK when people forget to change their address when
23 they move house, and they don't reregister their car,
24 but we cannot fine. And that is an issue. All we can
25 do is really cut people off and they lose the domain

1 name, and if they're really crooks, they just go and
2 relaunch with a different domain name.

3 So, that was just some thoughts that came from
4 the other speakers.

5 MS. MITHAL: Thanks. Other remaining people who
6 have tents up, I would like to ask people to focus on
7 the question of if, say, law enforcement said, look, you
8 know, we want to improve the accuracy of the whois
9 database, as registrars and registries, you know, what
10 can you do to help us? Can you implement the
11 recommendations in the Whois Task Force report, is there
12 anything you can do above and beyond that to ensure the
13 accuracy of data. I would like people to address that
14 point if they could.

15 So, let's have Dan and then Mike and then is
16 that Wayne?

17 MR. MacLAURIN: Sure.

18 MS. MITHAL: Wayne and then Jonathan. Why don't
19 we stop at Wayne and then we can go forward.

20 MR. SALSBURG: I think Willie raised a very good
21 point, and that's that the registrars do have an
22 economic incentive to ensure the accuracy of the data.
23 Otherwise, how are you going to know who to send the
24 renewal to, how are you going to know who to bill again?
25 And the question is that how do you ensure that this

1 accurate information that you may have in internal
2 databases, because you have that incentive, getting in
3 the external database that is viewable by others. And
4 do you collect this and keep it in essentially two sets
5 of books, or do you cross check it and try to ensure
6 based on the information you're collecting for billing
7 purposes that your whois data is accurate?

8 And, in addition, there are proactive steps that
9 it sounds like some of you already take in trying to
10 ensure that the whois data isn't just garbage. Do any
11 of you also do things like ensuring that zip codes match
12 addresses, those kind of basic things that at the very
13 least it will cure the honest person making an error.
14 It may not stop the actual person engaged in fraud, but
15 still, the person engaged in fraud from your own
16 economic incentive, they're not the ones that you want
17 to ensure that you can renew their registration, it's
18 the people who mistakenly missed a digit.

19 So, those are two questions for you. And I
20 guess I'll stop there.

21 MS. MITHAL: Okay, Mike?

22 MR. PALAGE: Yeah, just a couple of quick points
23 here. Within the past week, I've talked to three
24 registrars that have voluntarily begun to implement CVV2
25 and address verification, not because of what the Whois

1 Task Force recommended, not because law enforcement had
2 asked, but because of a business decision, they were hit
3 with tens of thousands of dollars in credit card
4 chargebacks.

5 So, as I said, I think Phillip here hit on a
6 good point, registrars, most registrars are as Paul
7 said, 160 registrars, each with its own unique business
8 model, but most of them are legitimate businesses trying
9 to provide a service and they are trying to have the
10 valid data to get renewals and stuff like that. And
11 some of the steps that they are taking to identify
12 inaccurate data I view as a positive step in the right
13 direction.

14 One of the things I think most registrars are at
15 times concerned with are unfunded mandates by third
16 parties, without a proper cost benefit analysis. And,
17 again, just an example to sort of follow up on what
18 Willie had mentioned earlier, good people wanting to
19 have accurate data, it took me last year and a half ago,
20 it took me three months of faxes and emails to get my
21 particular registrar to update the data. The data
22 wasn't updated, and my name was deleted -- well, it was
23 expired, I had -- it was quite difficult. And I
24 consider myself a good person who has accurate data.

25 And the change there was because of an email

1 change, which as Marilyn can say from her company, who
2 has had different carriers, there's been a lot of users
3 that have had numerous email changes. So, again, when
4 Willie was saying good people wanting to have accurate
5 data is true.

6 The one other thing about bad people being very
7 smart, and I think I had raised this with you was, I
8 recently was involved in working with a large
9 corporation that what happened was a certain
10 environmental group had an issue with a particular
11 chemical company, and they registered a protest site in
12 the name of the son of the president of the company.
13 They had his address, they had everything right. So,
14 again, you know, this was some place where the smart
15 people or the bad people are quite smart and sometimes
16 they could actually be quite ironic and devious all
17 wrapped up at the same time.

18 So, again, when you look at this, registrars, I
19 think, overall, want to have accurate data because it's
20 a business decision for them, they are just at times
21 concerned with unfunded mandate without the proper cost
22 benefit analysis. So --

23 MS. MITHAL: Wayne?

24 MR. MacLAURIN: To give you an idea of what this
25 actually costs us. The ICANN, Internet.Net mandate to

1 check whois, probably take us two to three hours per
2 incident to actually track down and verify from the time
3 we get the initial complaint and closing it on the
4 Internet. So, that's a pretty high cost for us to
5 assume, right? And we're happy to do it, because, as
6 you said, we want the information correct.

7 But it's not easy for us to verify that info.
8 Either manually or automated. Yes, it would be nice if
9 we checked zip codes, but that's easy, because the U.S.
10 has zip codes and a fairly well published database.
11 It's a little bit harder in Botswana, and much, much
12 harder in parts of the old Soviet union, where the
13 naming conventions are all over the place.

14 Even in the States, we can get a perfectly good
15 address in New York, and a phone number from Jersey. Is
16 that accurate or not? The fact is that the guy has a
17 cell phone that's been issued from New Jersey and it
18 works quite happily. So, this is not an easy thing for
19 us to fix or track or find. And I think you need to be
20 aware of that. There is no easy fix.

21 I know somebody who spent a great deal of time
22 and built a very big database trying to figure this out,
23 and it's on the order of gigs of data that they have to
24 mine to try to make a guess at a match. That's a
25 nontrivial exercise.

1 MS. MITHAL: Let me just follow up with a
2 question. You mentioned the cost for following up on
3 ICANN complaints that they refer. From a cost
4 perspective, are there any kind of up-front verification
5 methods that could save those post hoc costs down the
6 road?

7 MR. MacLAURIN: Well, certainly there are a few
8 ways to validate some of the information, right, and
9 there are some third party options you can do. There's
10 certainly some stuff you could do internally. One we
11 would love to do is to have the credit card companies
12 actually provide us a uniform method of checking
13 information. Visa is quite happy in the States to
14 verify card, address and zip code, I believe, that
15 doesn't exist anywhere else. Canada, it's card number
16 and expiration date.

17 So, there's no way for us to check to see
18 whether or not it's a fraudulent charge, even the fact
19 that it's the right information, the right card number,
20 we can't validate that. And so it -- there are some
21 solutions, but none that are particularly broad.

22 MS. MITHAL: I want to wrap up this discussion
23 on accuracy. So, the people who have tents are Kathy,
24 Ruchika, Chris and Jonathan. So, we can go in that
25 order.

1 MS. KLEIMAN: I know, Maneesha, that you have
2 drawn the distinction between commercial and
3 noncommercial, but the registrars at the table represent
4 both and my concern is always that the policies we adopt
5 for one should be clear as to who they apply to,
6 particularly if the intent is only to make them apply to
7 commercial, what is it going to do for those who are
8 using domain names for noncommercial.

9 Paul Kane has mentioned a solution that they've
10 come up with in the UK that doesn't really work
11 internationally, that if you want to protect -- that
12 domain name holders using their domain names for
13 noncommercial purposes have to go to a third party in
14 order to have any privacy. That third party will have
15 the liability probably for whatever speech they put on.

16 So, that's the last place that you want to go if
17 you're talking about human rights abuses, torture,
18 corruption, no third party is probably going to want to
19 take on the liability of hosting, or being the name of
20 representing that speech or being held out to represent
21 that speech.

22 I mean, people use the Internet to communicate
23 their own speech, they want to communicate directly.
24 So, accuracy and privacy go hand in hand really to me
25 and the idea of creating tiered access, and I was

1 wondering if anyone -- can I pose a question, because
2 there are technologies out there that are being
3 developed, including one by the IATF called CRISP, I
4 understand, that would allow kind of a tiered access and
5 allow people to obtain and opt out opt in and opt out.
6 So, the data could be accurate, but just not all
7 globally available at the same time.

8 MS. MITHAL: Does anybody want to respond to
9 that? People who have tents up. If you would like to,
10 you can. If not, that's okay.

11 MS. AGRAWAL: I was going to -- that's a good
12 question to pursue. I was going to ask two different
13 questions. I think the FTC should consider how the
14 global public sensibility of whois information actually
15 contributes to fraud, to identity theft, to spam, and to
16 some of the issues that were mentioned before. I think
17 that's an important study, and the FTC should see how
18 that impacts them from that sense.

19 The second question I want to read is if we were
20 to draw an analogy with the abstaining subscriber
21 information, law enforcement has to get a subpoena or
22 court order or search warrant to get subscriber
23 information. Why not apply that to domain name
24 registrants?

25 MS. MITHAL: Chris and John?

1 MR. DISSPAIN: Yeah, Chris Disspain from
2 Australia. I just wanted to -- the topic for discussion
3 is accuracy of the data, as I understand it at the
4 moment, not necessarily its availability, just the
5 accuracy. In Australia, we do much the same as the task
6 force has recommended, in that we insist that our
7 registrars contact registrants to check their data on a
8 relatively regular basis. And in any event, presumably,
9 even in the GTLD space, registrars contact registrants
10 when their domain name is up for renewal.

11 If you take Willie's point that the crooks are
12 going to lie anyway, and the good people want their data
13 to be accurate, is it not sufficient to have a situation
14 where if when you come to renew your name, you're
15 effectively warranting that your data is accurate, and
16 the registrars are simply checking to make sure that
17 they can contact you. If you can't -- if you can't
18 contact, you can't renew. If you can contact, then
19 surely that's sufficient. I don't see that there's
20 actually -- I think that solves the accuracy problem.

21 MR. BLACK: The crooks don't care.

22 MR. DISSPAIN: They don't care, exactly.

23 MR. BLACK: They'll make a warrant. I mean, if
24 they're going to steal money from people, they don't
25 mind warranting to you that it's accurate.

1 MR. DISSPAIN: The question is if we're talking
2 about accuracy of data, then as you say, Willie, good
3 people want their data to be accurate. People do not
4 walk down the street every day thinking of their domain
5 name, although it may sound, but they do think about it
6 when it's time to renew it, and at that point, you can
7 check the data. If what we're talking about here is
8 actually accuracy of data of crooks, that's actually
9 something slightly different, and that's much more
10 complicated to get to the bottom of.

11 MS. MITHAL: Jonathan?

12 MR. BAMFORD: Just to deal with a couple of
13 points as a co-op, and I know you don't want to deal
14 with a whole raft of privacy issues, but I'm not quite
15 certain that it's so easy to side step what falls into
16 data protection areas and what does not. Because I get
17 the impression that somebody operating on a domestic
18 basis is covered by a data protection and somebody who
19 operates on a commercial basis isn't. This isn't
20 actually true. If you're a living individual and you're
21 operating in a business context, data protection law
22 still applies to you.

23 So, anybody who operates as a data protection
24 consultant, Jonathan Bamford, data protection
25 consultant, there will be personal data about me, even

1 though I'm operating in a business context. So, it's
2 hard to park the sort of privacy issues to one side
3 there.

4 And the second point I would just make is that
5 in those instances where data protection law does apply,
6 and then one of the requirements is that personal
7 information is accurate and kept up to date. And so
8 it's not just a question of people being virtuous in
9 terms of keeping information accurate, there is actually
10 a legal requirement when it's personal data to keep it
11 accurate and up to date.

12 Reasonable measures to do that and extracts may
13 be some of the things that have been suggested there in
14 terms of updating it at a reasonable frequency, and
15 asking people may well be the reasonable measures, given
16 the nature of the information.

17 MS. MITHAL: Okay. I'll give Dan the last word
18 on the subject.

19 MR. SALSBURG: Thank you. One of the themes
20 I've heard from Willie and from others is that if the
21 data that crooks submit is going to be inaccurate
22 anyway, why even have this conversation, why do we care?
23 I think that there are two issues there. One is that
24 vastly overestimates the intelligence of the majority of
25 crooks. We have been highly successful in the cases

1 that we bring, using whois data as the building blocks
2 for our cases. That's the first point.

3 And the second one is that even in those
4 instances where we have found inaccurate data, when we
5 have been able to search along other fields, we have
6 been able to find patterns that have been able to tie
7 numerous websites together as being -- pointing to the
8 same culprit. For instance, same address, where there's
9 a same contact name, or even if it's a same false
10 registrant. The fact that there was a same registrant
11 and same false information has enabled us to put cases
12 together pretty quickly.

13 MR. DISSPAIN: It's about access to the data,
14 not the accuracy of it.

15 MR. SALSBURG: Well, it's both, clearly.

16 MS. MITHAL: Okay, thanks, Dan.

17 Actually we started getting into the CCTLDs and
18 what some of the policies are in the CCTLDs. So, I
19 thought we could start by just asking Michael Donohue, I
20 know the OECD is working on a report assessing some of
21 the policies of the CCTLD. So, Michael, can you
22 summarize or tell us anything about that report?

23 MR. DONOHUE: Again, not as much as I would
24 like, hopefully the report will be finalized in the next
25 few weeks and will be available on the website for

1 anybody who is interested.

2 UNIDENTIFIED SPEAKER: Excuse me, could you
3 speak into the mic, please.

4 MR. DONOHUE: Sorry about that. Is that better?

5 It's just a study of CCTLDs, the administration
6 of CCTLDs, and it's limited to the OECD countries, so
7 it's far from a survey of the whole world, but it does
8 show that there is an increasing -- registrations in
9 CCTLDs are growing at a faster rate than they are in the
10 GTLDs. They have doubled between July of 2000 and July
11 of 2002.

12 The rules and policies used to administer CCTLDs
13 vary quite considerably within the OECD. Although most
14 all of them have a whois function, the information
15 that's available in the whois function varies quite
16 considerably, particularly with respect to the contact
17 information that we've primarily been focused on, I
18 think, today.

19 Around 70 percent of CCTLD domain names in OECD
20 make the contact details available via whois according
21 to our preliminary information. So, there will be a lot
22 more in this paper, but I'm sorry, I don't have it yet
23 for you.

24 MS. MITHAL: Willie or Chris, do you want to add
25 anything to that specifically about .AU and .UK?

1 MR. DISSPAIN: Can I go first, Willie?

2 MR. BLACK: Yes, thank you.

3 MR. DISSPAIN: It may just help to give you a
4 very brief outline of what we do in Australia. We
5 introduced a new regime on the 1st of July last year and
6 that, in fact, led to a significant reduction of the
7 amount of data we make available in the whois. Our data
8 is relatively accurate on the basis that there are
9 significant policy hoops that people have to jump
10 through in Australia in order to get a domain name.

11 .AU is only used for companies, for example, for
12 people in business and so on, and it has to be a
13 connection between the registrant and the name. So,
14 from an accuracy point of view, because of the fact that
15 we have policy, unlike the GTLD space, which doesn't
16 have any, our data is actually accurate. Most of the
17 data that is inaccurate is inaccurate because, as I
18 said, people don't spend their time thinking about their
19 domain names until it comes time for renewal.

20 We actually have a redemption period if the
21 registrar tries to get in touch with you and your domain
22 name expires, you've got basically 14 days to renew it
23 before you lose it. You would be amazed at the number
24 of people who don't realize that their domain name is
25 not working for months.

1 But particularly, the availability of the data
2 is what I wanted to briefly address with respect to
3 Australia, and that is that we now simply say, show the
4 name of the registrar, the name of the registrant, and
5 an email address for the registrant to contact, and the
6 same for the technical contact. We do not provide an
7 address, we do not provide a telephone number, we don't
8 provide any other data. We have that information, but
9 we don't make it public.

10 Now, what we have, our equivalent of this body
11 is the ACCC, and we have an agreement with the ACCC that
12 they will send us a simple form if they want to find out
13 the information and we will give them the information,
14 to a degree. But we believe that to publish the
15 information so that literally anybody can look it up is
16 a recipe for disaster and has, in fact, been that in
17 Australia where the database has been misused, abused,
18 and people basically just got to the point where they
19 said we're not prepared to put up with it anymore, and
20 there is no circumstance here which I can see Australia
21 going back to a situation where full data is published.
22 It just isn't going to happen.

23 MS. MITHAL: Okay, thank you.

24 Willie?

25 MR. BLACK: Fairly recently, the UK is one of

1 the older top-level domain country codes. We've
2 probably been talking registration since the late
3 eighties, I guess. And some of the information was
4 fairly crude. And, in fact, up until very recently, we
5 just basically announced to the registrant laws, but
6 listening to other people around the world and in the
7 ICANN framework, and indeed folk who wanted to know a
8 little bit more information than intellectual property
9 consistencies, we decided that we would extend it.

10 Now, our first point is that we are trying to
11 get away from the old concepts of admin and technical
12 contacts. We believe that the technical contact is
13 associated with the service, and so that's one thing.
14 And the contact, the admin contacts, basically our prime
15 concern is who the registrant is, because that's who
16 we've got the contract with. And that can be a company,
17 it could be a partnership, it can be a sole trader.
18 There are many types of legal entities that can trade.
19 Or not. Or indeed contract, I think that's the word I
20 want to say.

21 So, we decided that we would publish the name of
22 the registrant and an address. We declined to publish
23 telephone numbers, fax numbers, or email addresses for
24 the obvious reasons that we don't want people being
25 phoned up and we don't want people being spammed with

1 their email addresses. We do have such information for
2 the registrant, but we keep that in our private
3 database. So, we have a database of all our registrants
4 with this extended information and we simply feed the
5 whois with the name of the registrant, and an address.

6 Now, in order to do this, we went through our
7 policy-making process in the UK, we have a policy making
8 board that contains both our registration agents, we've
9 got about 3,000 of them who are almost equivalent to
10 registrars, but there is a fine distinction, and they
11 elect certain people. We also have a consumers person,
12 we have a government department of trade and industry
13 person. We've got another eight stakeholder groups
14 involved in the policy board.

15 And the policy board discussed this, and we
16 actually went to wide consultation with the public, and
17 said, guys, we're going to public addresses, and of
18 course we had quite a few people saying, no, my teenage
19 daughter's address isn't going to be put up there. And
20 the stuff that Kathy was quite reasonably mentioning.
21 And so we did give them an opt-out, and the opt-out is
22 that they can use their agent, which is basically the
23 equivalent of the registrar, but only if it's a person
24 and they're not trading.

25 You see, in Europe we have another directive

1 called the distant selling directive, and that compels
2 somebody who is trading over the net to actually reveal
3 where they're trading from. And so even a sole trader
4 who is trading must declare where their address is on
5 their website, so therefore there is no down side to
6 them declaring it and us having it available in the
7 whois.

8 So, with all that, we made the change and we're
9 gradually rolling this out so that there will be an
10 address there.

11 With respect to revealing the extra information,
12 our data protection contractual terms allow us to give
13 it away to the authorities that would be making an
14 investigation, how formal that needs to be may depend on
15 where the request is coming from, because obviously we
16 don't want to be giving away the information to somebody
17 pretending to be doing an investigation who really
18 isn't.

19 And so there is an issue there, I'm sure we'll
20 get around to things like that later. But just before I
21 stop, I want to point out that I'm also chairman of
22 CENTA, which has got 30-odd other CCTLDs there, and I
23 notice this whole meeting has been rather Anglo-Saxon
24 oriented, if you don't mind me saying, we've got some
25 German colleagues here, but for the most part, it's

1 been, if you like, the common law countries, Australia,
2 Canada, the U.S., the UK. And, in fact, within CENTA,
3 we have, of course, other EU members, but we've also got
4 the former Eastern Block, you know, the Polands, the new
5 Europe, that's right. To make a topical diversion,
6 thanks, Chris.

7 And, actually, we have even a member from Iran.
8 Now, you've got surreal countries and you've also got
9 many other countries in the whole panoply of the CCTLD
10 world that don't actually quite have the same
11 contractual view of life, and that don't have quite the
12 same views of privacy, and some of the issues that
13 western democracies may value.

14 So, we've got to remember that even within the
15 Channel Islands, they have quite a distinct kind of
16 thing that they're near France but yet they're part of
17 the British Isles, but they're not part of the United
18 Kingdom and they're not part of the EU, but they copy a
19 lot of our internal stuff from both the EU and they've
20 got some of their own.

21 So, do remember that although we're talking here
22 basically about common law countries and the general
23 contractual framework that we live in, the world of
24 CCTLDs is quite diverse. So, that was just a little
25 point I thought I better make.

1 MS. MITHAL: Thank you, Willie.

2 I would also like to ask if Wayne or Henning,
3 you have any comments to add about .DE or .CA.

4 MR. MacLAURIN: Sure, the CA world has actually
5 sort of gone back and forth. Back in the good old days,
6 pre-competition, pre-anything else, it was actually
7 pretty hard to get a CA domain. First of all, you had
8 to figure out who was selling them, which was a
9 nontrivial task. And then they had the rules where if
10 you were a corporation, you could have -- if you were a
11 Canadian corporation, you could have .CA; if you were a
12 provincial corporation, you got sort of a geographical,
13 just .ON.CA; you know, Ottawa.ON.CA, if you happened to
14 be personal.

15 So, all this was a little bit easier, because if
16 you were a Canadian corporation, you showed up in the
17 Canadian corporation database and it was kind of easy to
18 validate that that's who you were.

19 They've gone kind of the other direction since
20 then and although they still require you to define what
21 you are, if you're a Canadian corporation or anything
22 else, the domain itself is relatively open. So, we can
23 still validate some of the information in terms of if
24 somebody claims to be a Canadian corporation, we can
25 validate that, but it still leaves it wide open if you

1 came to an individual, for example.

2 Our CERA, who is our overseeing body, does check
3 the information and they do submit requests for
4 validation on a regular basis as part of their ongoing
5 registration process. Fairly like Australia does as
6 well.

7 MS. MITHAL: And what fields of data are
8 available?

9 MR. MacLAURIN: It's a lot like whois, although
10 it is a fat whois, in terms of it's controlled by CERA.
11 They do show the registrant, the new contact and old
12 contact information, address phone numbers and email.

13 MS. MITHAL: Thank you.

14 Henning?

15 MR. GROTE: In the ENUM space, it's a bit
16 different, it's quite -- it's been changing now. The
17 data that is available is restricted, not when it comes
18 to access, but to the number of different data fields
19 that are shown. And right now I just received the
20 actual -- I don't know the exact English expression, but
21 the -- when it comes to privacy, the data protection
22 commissioner of the federal state where the DE Nic, the
23 top authority for the DE name space is situated, is
24 located. This chief commissioner just issued his report
25 about a privacy data protection in the DE name space,

1 and there the opt-in is asked for.

2 So, that means for living, breathing
3 individuals, I like that expression for private persons,
4 there should be provisions for an opt-in in the whois
5 database. That means if they don't use the opt-in
6 option, there won't be any further information than just
7 the name of the registrant, as I interpret it. But we
8 have to go deeper into that issue, it's not implemented
9 yet. It's still on.

10 I think hearing these comments from some of the
11 CCTLD representatives, it seems clear that the policies
12 vary pretty widely among CCTLDs, and I know, Marilyn,
13 that the Whois Task Force was looking into this
14 uniformity issue, and I'm wondering if you could just
15 tell us what happened on that.

16 MS. CADE: In relation to -- let me -- one of
17 the questions we ask, several questions we asked had to
18 do with uniformity and consistency of data elements, and
19 then separately, we asked questions about searchability.

20 The task force was very much taking the point of
21 view that accuracy can be separated from access, and I
22 think we're hearing some examples of, in fact, where
23 accuracy and access are related to each other, but not
24 necessarily a one-to-one match.

25 In the consistency of data elements, we will be

1 putting forward an issues report which is likely to say
2 that uniformity and consistency of data elements needs a
3 sort of wait and see approach before implementation.

4 Certainly there's standards work that is going
5 on that needs to -- would call it ripen further, and
6 anybody in this room who has been involved in standards
7 knows that there's the development of the standards and
8 then there's the publication of the standards, and then,
9 oh, there's the adoption stage of the standard. So,
10 just because we're making progress on getting standards
11 matured, I would say in the development process, we've
12 still got a ways to go.

13 So, the issues report will recommend that people
14 work more actively within the standards process. In the
15 issues of searchability, the issues report is likely to
16 say that in the implementation of consistency and
17 uniformity of data elements, and in searchability, that
18 there can be increased challenges with possible
19 profiling if there are not protections implemented at
20 the same time.

21 So, that is sort of on hold. We did -- or will
22 be, I think, recommended to be on hold. We did look at
23 and asked the question of do you expect uniformity and
24 consistency of data elements in CCTLDs and in GTLDs, and
25 there's strong support for uniformity and consistency of

1 data elements across the GTLDs and also in the CCTLDs.

2 In our conversation with CCTLDs, I think what we
3 were hearing, and we did talk to some, we talked to
4 Canada, we talked to Mexico, we talked to a couple of
5 others, there are CCTLDs who actively do data checking
6 before they enter data. Most of the CCTLDs, and maybe
7 Paul might want to comment on this, are really looking
8 for effective software applications, and so the feedback
9 we got was we'll be waiting, like everyone else, to see
10 if there's a useful standard, and when the standard is
11 available, then we'll be interested in considering
12 deploying it, but it doesn't seem to be something we
13 would leap into right now until the standard is
14 available.

15 MS. MITHAL: Thank you, Marilyn.

16 I'll call on the two of you next, but I just
17 wanted to ask Chris Disspain a follow-up question, and I
18 should mention that Chris came in from Australia last
19 night, he is leaving at 4:00 today to go back to
20 Australia. In fact he has to leave at quarter to 4:00,
21 and so I want to make sure to get in all my questions to
22 him. I think he wins the prize for dedication to this
23 workshop.

24 MR. DISSPAIN: Actually I didn't come in last
25 night, I did stop in LA. I was forced to stop in LA.

1 due to snow.

2 MS. MITHAL: Thank you for coming.

3 MR. DISSPAIN: My pleasure.

4 MS. MITHAL: To follow up on something, you said
5 there were not publicly available information in the
6 data fields to the public, and I guess my question is
7 let's say the FTC, for example, were investigating an
8 Australian website that was targeting U.S. consumers
9 that ended in .AU, we didn't see that information in the
10 whois database. Is there any way we could access that
11 information?

12 MR. DISSPAIN: Well, I guess there's several
13 ways that you could access that information. I imagine
14 that you have some kind of arrangements or consult
15 talking to your equivalent in Australia about all sorts
16 of things, and I have no doubt if you ask them if they
17 would ask us, then they probably would. If you asked us
18 yourself, I don't actually -- it hasn't happened.

19 I guess the answer would be that -- see, it's
20 complicated by this particular point: If we were
21 investigating -- if the Australian authorities were
22 investigating something in the States that was illegal
23 in Australia but legal in America, how would that pan
24 out for you, and the same way that if we -- if what you
25 were concerned about wasn't actually a problem for us,

1 I'm thinking, for example, about pornography, as an
2 example.

3 I mean, we have what our government likes to
4 refer to as content legislation, where most of us refer
5 to as a complete and utter waste of time, but
6 nonetheless, they seem to think it's important. And if
7 we were trying to get hold of some information about
8 U.S. people who were doing things that weren't
9 necessarily illegal here, how would that work, from your
10 point of view?

11 So, it's a very complicated question to which
12 there is not a simple answer. If we get a request from
13 our authorities, then we will obviously provide that
14 information to them.

15 MS. MITHAL: I think we're going to follow up on
16 some of these issues a little more after the break, but
17 I just wanted to get Chris' perspective before he had to
18 take off. So, let's have Paul and then Mike and then
19 Ruchika, and then that will be the last word on this
20 issue.

21 MR. KANE: Thank you, Maneesha.

22 Just again a few more statistics. There are 244
23 country code top-level domains, of which 118 have online
24 whois databases of one sort or another. We have learned
25 that various registries, CCTLD registries, publish

1 various data elements, and we've also just learned, and
2 it's very obvious that the registries have to abide by
3 the law of the country in which the registry is based.

4 And so, whereas there is no get-out for criminal
5 activity, there is, I think it's fair to say, within all
6 data protection legislation, if law enforcement asked
7 for information and provided the appropriate
8 documentation, then whoever holds the information must
9 provide it to the respective party. But it means in the
10 international context, probably, and I'm guessing, as
11 Chris was referring to, that one had to go to the ACCC
12 and ask them to get the information rather than anyone
13 else.

14 But the point I really wanted to make was to
15 highlight, as Willie alluded to earlier, the different
16 relationships between CCTLDs, the registrars and the
17 registrants. Willie is able, in the UK, Nominet, the
18 relationship is with the registrant. The registry has a
19 direct contract with the registrant. In GTLDs -- and
20 therefore Nominet, let's say, owns in the broader sense,
21 the data.

22 In the GTLD space, there's a difference, insofar
23 that the registrar may, in certain circumstances, own
24 the data. And so, and we have an agency relationship
25 where the registrar may be an agent of the registrant,

1 in some jurisdiction, or the registrar may be an agent
2 of the registry.

3 So, there are a whole range of different areas.
4 In terms of searchability and having some uniform
5 format, a few years ago I was the European
6 representative of the registrars when in Germany, the
7 Federal Data Protection Office wanted to jump on all
8 German registrars because they considered the provision
9 of bulk whois information, which accords with the
10 registrar/registry agreement, was in violation of German
11 data protection law.

12 And that would obviously have created a bit of a
13 political situation. And fortunately, we were able to
14 smooth the waters. Subsequently, there are other
15 restrictions in Europe and elsewhere which are trying
16 not to go down a uniform approach, which I find a great
17 shame. It would be great to have a uniform manner, but
18 one of the issues is if this is pushed rather hard, and
19 reference was made to searchability, one of the fears
20 would be that enabling data to pass across national
21 frontiers, in a searchable format, could present
22 significant challenges within the European Union area,
23 within Argentina, within Israel, within Japan, and cause
24 a fragmentation of this thing that we are trying to keep
25 united, the whois.

1 And so in CCTLD land, where registries must
2 abide by national law, one needs to be very sensitive to
3 the fact that registries' first duty is one accord to
4 national law, but also to try to have this uniform
5 framework. If one tries to have lots of searchability
6 that the gentleman is referring to, yes, it was great in
7 GTLD land, but one needs to be very, very sensitive to
8 the various requirements within CCs, because otherwise
9 people will start shutting down, as Austria -- I'm
10 sorry, Australia has done, and I really want there to
11 be, as I was discussing with you yesterday, the concept
12 of having differential access for different parties
13 brings a whole rash of problems.

14 One, you have to identify who the owner of the
15 data is, and two, you have to identify if it's an
16 appropriate agency that's making contact. And so if
17 anything, it will frustrate law enforcement, who are
18 actually trying to help and trying to get the bad guys.

19 MS. MITHAL: Thanks.

20 Mike?

21 MR. PALAGE: Actually, that was actually an
22 excellent segue. Going back to what Commissioner
23 Swindle said earlier today about I don't want to hear
24 about the problems, I want to hear about solutions to
25 solving the problems. Following up on what Paul just

1 said, there's 160 registrars in a number of
2 jurisdictions. It is very difficult for them if they
3 were to receive something from the ACCC from Australia,
4 they would say, who is this.

5 It really represents an alphabet soup of
6 agencies which makes it rather difficult for registrars,
7 and as Phillip said, there is a lot of small, mid-sized
8 registrars that think this is very complicated. One of
9 the ideas that I would like to throw out, and maybe this
10 is something the FTC could bring up with their GAC
11 representative within ICANN, is that, what is it, about
12 a year and a half ago, ICANN passed board resolution
13 0192, which dealt with the country names on the ISO 3166
14 list in the .info space. And what happened there was
15 the ICANN board basically said take these country names
16 and make sure that the appropriate government agency can
17 register it.

18 Now, that sounds real easy, but one of the
19 things in ICANN is when something sounds easy, actually
20 implementing it becomes quite difficult. And one of the
21 things that I have been working with is a consultant
22 with Afilias who is trying to identify who can speak on
23 behalf of Germany.info.

24 And, again, to use the example, there were
25 actually two names on the list, Germany and Deutschland.

1 And the system that was put in place was that if there
2 was a request from a government saying I want this name,
3 what Afiliias or what ICANN did was they would contact
4 the GAC representative -- they would contact the GAC
5 secretariat and then ask the secretariat to go to the
6 appropriate government and say, who within your
7 government can speak for this domain name? Who would be
8 eligible to register it?

9 So, that actually from Afiliias' standpoint
10 provided somewhat of a uniform standpoint to make sure
11 that the right person got it.

12 And I guess this is what Paul was saying, is if
13 maybe the governments were to work to identify who is an
14 appropriate law enforcement agency, because again, you
15 wouldn't want some potential sheriff in Podunk, USA
16 trying to have access to, you know, data. Again, you
17 need to have sort of a tiered access approach.

18 And I think that's one of the ideas you may want
19 to consider of how to use the GAC in a constructive
20 manner to make it simpler for registrars to work with
21 law enforcement in addressing these situations, while
22 simultaneously going towards what I propose, which is
23 sort of a tiered access to the whois, where you have law
24 enforcement, the intellectual property or business
25 community, and then individual registrants. I think

1 that that tiered approach is part of what a long-term
2 solution is.

3 MS. MITHAL: Thanks, Mike, and I think I would
4 really take both of your points about, you know, how to
5 know whether a law enforcement agency is who they say
6 they are, and I would like to kind of save that
7 discussion for after the break.

8 Ruchika had her tent up and if we could just
9 close the discussion on accuracy and searchability of
10 whois data.

11 MS. AGRAWAL: Well, I am on the Whois Task Force
12 as a noncommercial constituency representative and I
13 work for the Electronic Privacy Information Center. I
14 am going to put on my techy hat for the moment and I am
15 going to talk about a new protocol that's being
16 discussed by the Internet Engineering Task Force and
17 that's called the EPP, and basically it's going to
18 standardize whois data and it seems to speak to
19 uniformity. I think it seems to me that many of us at
20 this table should probably think about the issues and
21 the questions that's going to raise for many of us, and
22 I'm not sure if Marilyn wants to address the uniformity
23 issues report, if we're talking about the EPP protocol
24 and how that may impact our issues report.

25 MS. MITHAL: Do you want to respond?

1 MS. CADE: It's CRISP. We should just clarify
2 the EPP protocol is a registry protocol, and there's a
3 discussion within the IETF Task Force about whether or
4 not to add either extensions or tagging to each of the
5 elements, but CRISP I think is the protocol that we've
6 been talking about the IETF developing, which could lead
7 to uniformity for whois.

8 Both of those would clearly have -- but again,
9 it comes down to how is it implemented, because you
10 could certainly have a standard which has capability,
11 but not turn certain features on in the implementation.
12 And as we heard in the Whois Task Force, and everybody
13 here who works on the IETF is probably tired of hearing,
14 there's technical standards and then there's all this
15 policy stuff. And the policy stuff seems to always
16 impose into the technical standards.

17 Again, I think in our report, what you are going
18 to mostly see us say is there are a lot of questions,
19 and they need to be really thought about, because
20 implementation would be done in one way and might lead
21 to the ability to have easier data profiling, and
22 implementation could be done in another way and
23 searchability would be there, but it would not be a
24 feature that was turned on unless it was authorized
25 access.

1 MS. MITHAL: Thanks, Marilyn.

2 Okay, well, let me just summarize this
3 discussion, and I just think that I've taken maybe three
4 points out of this, three main points. One is that
5 there are privacy issues, and we need to continue to
6 work together to figure out how to deal with those
7 issues, and so we should have continued dialogue there.
8 I think there's general agreement at the table that law
9 enforcement, bona fide law enforcement, should have
10 access to accurate whois data, but we need to keep in
11 mind costs on registrars that, you know, that we might
12 impose if we require them to do too much in the way of
13 checking accuracy.

14 So, with that, why don't we take a ten-minute
15 break, and I would ask everybody to come back at ten to
16 4:00 for the remainder of the discussion. Thanks.

17 (Whereupon, there was a recess in the
18 proceedings.)

19 MS. MITHAL: Okay, welcome back. As I mentioned
20 before, we'll spend probably until about 4:45 or so
21 talking about cooperation, and why don't we spend the
22 first half or so talking about cooperation and
23 information sharing and then we can talk about
24 cooperation in suspending fraudulent activity on
25 websites.

1 So, I thought it might be useful again to hear
2 from Dan to set the stage a little bit about the types
3 of information that we would be asking registrars and
4 registries for.

5 MR. SALSBURG: Let me start off by saying that
6 the frauds that we see often involve multiple websites.
7 So, what you will frequently see are a number of teaser
8 sites that have some sort of claim that feed into some
9 central sites that may be the sites for their billing,
10 the credit card information is collected, or there's a
11 fulfillment page where additional information would be
12 taken for sending out the materials or for just
13 collecting personal information that will then be
14 traded, without the consumer's knowledge.

15 So, keeping that in the back of your mind, the
16 types of frauds that we're looking at. The types of
17 information that we see from the whois database is
18 pretty varied. We're not just looking for the name of a
19 registrant. We are looking at any ways that we can put
20 together all the different elements of a scam. And that
21 means that we frequently are trying to find websites
22 that are registered to the same address, the same
23 registrant, obviously, the same contacts, administrative
24 or technical contacts, street addresses.

25 I alluded to before that up until several months

1 ago, at least with Verisign, we could search across the
2 registrant's name field, which was a very helpful
3 investigative tool. That unfortunately has changed, we
4 can no longer do that. We are left right now with
5 issuing civil investigative demands or CIDs, which are
6 our version of administrative subpoenas, to registrars
7 for getting information across these multiple fields.

8 Unfortunately, we all know, or I guess
9 importantly, the beauty of the Internet is the speed of
10 it. It's the ability to engage in commerce
11 instantaneously. The downside of this is that frauds
12 can operate instantaneously as well, and when we send
13 out a civil investigative demand, and we get back a
14 result four weeks later, which gives us some useful
15 information that we can then use to send out additional
16 civil investigative demands to other parties that might
17 need that information, we are so way behind the
18 fraudsters that it's getting very difficult to have in
19 many of our cases any chance of meaningful success in
20 Internet fraud investigations.

21 MS. MITHAL: Thanks, Dan.

22 And I think just to add to that, I think I have
23 discussed with a lot of you in prior conversations that
24 we often serve these civil investigative demands on
25 domestic registrars and we get cooperation from them,

1 but then we have the added complication of when a
2 registrar is located in another country, how can we get
3 cooperation.

4 And I think before the break, two ideas were
5 mentioned, Chris mentioned the idea of organizations
6 like the FTC going through their counterparts in the
7 other country, such as the ACCC in Australia, and then
8 Mike Palage mentioned the idea of having a government
9 contact list so that registrars could know who law
10 enforcement agencies are.

11 I think the one issue that Dan mentions that I
12 would like to ask everybody to think about is the need
13 for speed in this area. And I think it's a very good
14 point that we should strengthen our relationships with
15 governments across borders, but sometimes we just need
16 to move so fast. So, I'm wondering if we were to call
17 you, one of you who represents a foreign registrar, and
18 say, look, we really need this information very quickly,
19 is there any way you could voluntarily respond and what
20 are the constraints to responding voluntarily to that?

21 Phillip?

22 MR. GRABANSEE: I think one has to differentiate
23 between the practical and theoretical side here.
24 Certainly you can respond in an informal way and solve
25 the problem. Especially, you know, from a Continental

1 European or maybe from a German legal background, was a
2 legal system which doesn't have the threat of punitive
3 damages, and all those things involved, the legal fees
4 that are not as high, the losing party has to bear the
5 expenses, it has to pay the expense of the winning
6 party.

7 So, if you just give some information in an
8 informal way, as a lawyer, consulting registrars, if
9 they get a call from you, I would say just take a look
10 at the site and is there some truth to what the FTC is
11 saying, take the site away and probably nothing happens
12 and then you can say, okay, they're never going to sue
13 you anyway. So, it's a very practical solution.

14 But if you look at it from a theoretic
15 perspective, then it gets extremely difficult. And I
16 think that goes in the direction of the second question
17 part of the discussion, but other agencies or agencies
18 or courts outside Germany or outside from a different
19 country, it is very -- there is a recognition of foreign
20 rulings from courts or from agencies, this is a very
21 difficult question. You know, legally you don't have a
22 very strong meaning in the other jurisdiction.

23 So, if you take away a domain or give
24 information just on a court order from a foreign country
25 or just a request from a foreign agency, you have no

1 legal justification to do that. And of course you can
2 implement that maybe in the agreement that you had with
3 the registrant between the registrant saying we do give
4 -- we'll provide information if we've been requested or
5 we will cancel domain names, but then you face another
6 problem that I think that's a point that Paul Kane just
7 mentioned, the description of the legal relationship
8 between the registrar and the registrant, because if you
9 put this in the agreement as the registrant and have the
10 justification to give out the information, you have to
11 establish some kind of legal relationship between the
12 registrar and the registrant, and practically, that
13 doesn't work very often, because in between you have the
14 registrar and then you have the reseller and then an ISP
15 and then you have the registrant.

16 So, not very often do you really have a valid
17 contractual relationship between the registrar and
18 registrant, and for example German law, if the judge
19 would look at this relationship he would say it's
20 probably not valid to give justification to give the
21 domain names away.

22 So, on a theoretic way, it's very difficult and
23 probably only mutual legal aids or legal help agreements
24 can solve this problem. But I think a practical way is
25 if the FTC works together with consumer protection

1 agencies or what we have in Germany, half private, half
2 public consumer associations, as we call them, who has
3 the right of action, have the right to go to the United
4 States and as an entity to go to courts.

5 So, if the FTC works together with those on an
6 informal basis, works together with those entities and
7 those groups, this is a much more effective way, because
8 as we all know, to have mutual treaties to take care of
9 the problem, we probably will not have before we have
10 this established, we won't have the Internet in the way
11 it exists now for probably only another 10 or 15 years.

12 But working together on this in an informal way,
13 I think it will help and probably will be the best for
14 the consumers.

15 MS. MITHAL: So, what do people think of this
16 idea of informal cooperation?

17 Henning and then Willie?

18 MR. GROTE: Well, I have to totally agree with
19 Phillip, because well, of course, we are of the same
20 German experience and background. Just adding a few
21 things to what Phillip just said. In the practical life
22 goes with the informal way, no doubt. There still is
23 kind of this uncomfortable feeling because while you
24 have to know Deutsche Telekom is the world's largest
25 teleco, we are regulated in Germany, and very strict,

1 and so we're always under scrutiny.

2 As one registrant, it might be different. It
3 might be a different experience than that. But
4 nonetheless, to take on the broader picture, we rely
5 totally on consumer confidence. On that -- on the one
6 side, it's the privacy, the data protection, of course,
7 but the other side is a functioning law enforcement in
8 case, just in case.

9 So, we, like I say, for our company, we are
10 very, very happy to cooperate with the law enforcement
11 agencies, and even we have installed, of course, a
12 24-hour hotline for all law enforcement in Germany. So,
13 we are back now at the challenge. The whole thing, the
14 whole issue would be much more easier and much more
15 comfortable for everybody if we had a much more
16 formalized cooperation. Should it be worth the example
17 Phillip just mentioned, the kind of public/private
18 association, whether it's a mutual treaty between the
19 FTC or somebody else, or a multinational agreement,
20 multinational treaty when it comes to e-commerce. There
21 are lots of different initiatives going on on the
22 political stage.

23 So, it might very well be that one of these
24 building blocks can be used for that. So, we would be
25 too happy to assist on that issue.

1 For an example, from the practical side, right
2 now, when it goes to the usual way of legal -- mutual
3 legal assistance, I was told by our lawyers and the data
4 protection professionals at our headquarters that these
5 cases usually take weeks and months to complete. And
6 they were very, very happy that in the aftermath of
7 9/11, chasing an individual, everybody, the American
8 official sides and the German ministries and all that,
9 they were very proud that they managed the issue in a
10 few days.

11 So, this is not speed. So, we would like to
12 welcome the law enforcers. We have provided processes
13 within our cooperation. We do have law enforcement
14 hotlines, the only thing we need is a more formal
15 framework. We will work informal, of course, but we
16 need a formal framework for that.

17 MS. MITHAL: Willie?

18 MR. BLACK: Yeah, as my company lawyer would
19 say, but as a director of the company, I would be
20 concerned a little bit about informally giving it away.
21 Reminding people, again, of our data protection is
22 actually criminal. This is not just a civil -- my
23 protection expert here might correct me, but if somebody
24 were to challenge us, having given away their data
25 wantonly, without doing due diligence perhaps on who was

1 sending in the request, then it would possibly fall as a
2 criminal charge against the directors of the company.
3 And I certainly don't particularly want to be taken
4 along that route.

5 So, informally, I don't think it will work. I
6 think if there was an emergency and we had some
7 knowledge that it was a competent body that was
8 requesting it, we might be okay. I mean, our terms and
9 conditions say very clearly that we may provide your
10 personal data to governmental or law enforcement
11 agencies at their written request in connection with the
12 conducting of any investigation.

13 And that's what would govern it. Of course,
14 what is a legitimate reason? What is an investigation?
15 We've talked about this earlier. But for sure, if you
16 were to issue an administrative subpoena, I wouldn't
17 know it from an ice cream wrapper, to be frank, and I
18 don't think my lawyer would, from what she said here,
19 because she doesn't know what a U.S. administrative
20 subpoena is.

21 On the other hand, we know what something would
22 be in the UK, and I think if you're trying to get speed
23 here, that the best thing we could do is have a network
24 of cooperating agencies in each country whereby the
25 person requesting the information with some urgency

1 would, let's say, go to the FTC in the U.S., the FTC
2 would correspond rapidly with the Office of Fair Trading
3 in the UK, the Office of Fair Trading would have some
4 means of informing us and we would know who they were.
5 And that would mean that there would be a fairly quick
6 path through, and you can do this by authenticated
7 emails using digital signatures or something, and I
8 think this might just be possible to speed up things.

9 MS. MITHAL: Willie, I was going to follow up
10 with a question. I take it your point about not knowing
11 an administrative subpoena from what?

12 MR. BLACK: Oh, whatever. An ice cream wrapper.
13 I'm sure it's got a nice crust on it.

14 MS. MITHAL: Ice cream wrapper. I guess my
15 follow-up question would be, let's say you know Dan
16 Salsburg now and Dan picks up the phone and says Willie,
17 we really need some information here, can you give it to
18 us, and your privacy policy says we do share information
19 with law enforcement and investigators, what would be
20 the concern there?

21 MR. BLACK: If I thought it was Dan, then fine,
22 but I don't know that it's somebody pretending to be
23 Dan.

24 MR. SALSBURG: What if it was Maneesha?

25 MR. BLACK: Yeah, it can work, but you can set

1 up any pair of workable propositions, but it isn't just
2 going to be you and me. It's going to be my lawyer or
3 one of my customer support people that gets the first
4 query, and it's not necessarily going to be always the
5 U.S. and UK, it could be the Isle of Man or it could be
6 Chechnia or Romania. And the real issue is how do we
7 know. That's why I think setting up an N plus M, the
8 mathematician in me, you don't want an N times M
9 problem, because with everybody having to go to
10 everywhere else.

11 So, if you can set an M plus N problem, then we
12 all deal with our own agencies and the countries have a
13 network between them. And then it's a three-stage
14 process, of course, to go through it, but at least it
15 would have some certainty, and I think we would all feel
16 more comfortable. Because we have responsibilities. We
17 have duties and care to the registrants that we consider
18 very important as well. The genuine people that
19 somebody just doesn't try to rip them off by pretending
20 to be the FTC.

21 MS. MITHAL: Can I ask Jonathan to respond? And
22 then I will call on Marilyn and Phillip and Kathy and
23 Dan.

24 MR. BAMFORD: Okay, thank you.

25 I think I'll make a number of observations that

1 basically I think any arrangements which are founded on
2 the old pall sacks, as we call it in the UK, are fraught
3 with difficulty. I think you should formalize your
4 arrangements in the proper contact points. I think
5 there are areas that have to do with criminal policing
6 and these pressing times at the moment, things could be
7 put in place to ensure that things happen in an
8 expeditious way.

9 I wouldn't believe it's beyond the wits of
10 anybody in this room to establish quick arrangements
11 given the modern communications which we have available
12 to us, which apparently somebody can use but we struggle
13 with ourselves to use in some ways. I'm sure we can
14 manage to do that in an expeditious way through a
15 contract where then the particular community has
16 confidence in it being a properly routed request.

17 We have got plenty of experience in the UK in
18 the past where these sorts of arrangements, where named
19 individuals contact each other and for the exchange of
20 information, it turns out somebody, one of the named
21 individuals, has left the organization and is working
22 for tracing agents and bodies like that and the
23 information is finding its way to other areas. You
24 might leave tomorrow for all I know, you might be
25 sanctioned for gross misconduct, I have no idea. I'm

1 sure you won't.

2 MR. SALSBURG: But you don't know.

3 MR. BAMFORD: But I mean that's the point.

4 You've got to have confidence. And a desperate action
5 contact, even though Willie has made some statements
6 there and the terms and conditions of which you will do
7 business with people. He has to have reasonable grounds
8 for believing that those conditions are met. And what's
9 the level of reasonable grounds that he has?

10 Now, maybe tomorrow he might have some
11 reasonable grounds when he gets a phone call from you,
12 but in a month's time, I'm not quite so certain. But
13 anyway, just anybody over the telephone without the
14 backdrop of some official documentation is asking for
15 trouble in any event, because you need some way to
16 confirm just why you did it in the end.

17 I think a contact point in a country is a
18 sensible way of proceeding on the basis of comparative
19 organizations, and that strikes me as an easier way in
20 data protection terms than because of Willie in the UK
21 is then satisfying the demands of a local agency other
22 than an agency in a third country who he doesn't
23 necessarily know from anybody else. It could be, you
24 know, the Iranian consumer protection agency are on the
25 phone to him as much as it could be the Federal Trade

1 Commission.

2 MS. MITHAL: Thanks, Jonathan.

3 Marilyn?

4 MS. CADE: I want to first of all set the stage
5 by saying how sympathetic I am to the problem that is
6 faced, that the FTC is describing by sharing a situation
7 that we dealt with right before Christmas during the
8 shopping season when at 6:00 p.m. on Friday night, a
9 website went up and it was called AT&T-global.net and at
10 6:20 we detected it ourselves and recognized it as not
11 being a valid AT&T site.

12 The website was communicating with AT&T
13 subscribers and telling them that due to a D-DOS attack
14 and other corruption that had taken place, their
15 subscription information had been lost and they should
16 go to this AT&T authorized page which, oh, by the way,
17 was a direct replica of our customer service page and
18 fill in their personally identifiable information,
19 revalidate their credit card numbers, and by 8:20 we had
20 taken the site down by getting a DMCA compliant notice
21 sent to the ISP.

22 By 12:00 the site was back up on Friday night.
23 And we got it down again on Saturday morning, there was
24 a second ISP with a second DMCA compliant notice and it
25 went up again on Saturday night. And it was up all day

1 Sunday. We in the mean time had taken a number of steps
2 to notify all of our customers, and we don't like
3 telling our customers that they are the victim of fraud.
4 They trust us. We don't invest in the world's tenth
5 most well known brand for nothing. This is supposed to
6 be a secure and reliable system that we operate.

7 We, of course, are very dependent, and by the
8 way, the whois data was it appeared that it could be
9 correct, it was a gentleman who happened to live in
10 Ohio, oh, my God, once we found him he just happened to
11 be in Bulgaria. The story behind this is that we are
12 very dependent on being able to use whois ourselves, and
13 to protect our customers ourselves, and very dependent
14 on cooperation with the FTC and with their counterparts
15 in other countries.

16 I say that and at the same time we are very
17 cautious about informal arrangements. So, I would lend
18 my support to the need to find a way to have an
19 identified set of agencies. That's something, while I'm
20 not promoting the safe harbor as a model, I might
21 promote the concept that countries that you know in any
22 country who to go to. If you have a company in the U.S.
23 who appears to have violated the privacy of a European
24 citizen, then there's a place to go for that country
25 from the data privacy commission from the other country

1 can come to the FTC and there can be a contact with the
2 country, with the company in the United States that's
3 recognized. We know who the FTC is.

4 It seems to me that we ought to be thinking
5 about those kinds of models. Is there something in an
6 adjacent industry sector that could be built on or
7 created in a different way, is there a way to create
8 this network of agencies, but to formalize the
9 relationships.

10 We believe very strongly as an ISP, our terms of
11 service are very clear. If our customer violates our
12 terms of service, we have the right to deny them
13 service. And I think that's something that I appreciate
14 the problem that today is registrars may have in their
15 distribution channel, but maybe that's something that
16 they should really think about.

17 If the kinds of fraud continue on the Internet
18 that are going on now and the scams that are going on
19 now involving domain names continue, I regret to tell
20 you as registrars that you, too, will have to employ
21 close to 40 people to operate an enforcement desk, and
22 there are better ways to spend your money.

23 MS. MITHAL: Thanks, Marilyn.

24 Phillip and then Kathryn.

25 MR. GRABANSEE: I just wanted to make it clear

1 that certainly as a lawyer I am not advocating solving
2 things in an informal way always, this is not just
3 considering an academic discussion, also, you know,
4 describing a little bit of reality how things can be
5 sometimes practically solved. I just wanted to describe
6 that certainly we would all search for a formal better
7 structured way, especially for bigger companies who are
8 exposed more to the public, it's certainly a problem.
9 They will still solve problems informally but they
10 probably won't tell in discussion like that saying how
11 they do that.

12 But I have to come back to the question about
13 the administrative subpoena, what happens if that is
14 served with them and if it makes a difference if it's
15 really issued from you guys or from third parties, it's
16 not true. It might be a moral difference for a
17 registrar who receives it, is it really a real subpoena
18 or is it, you know, a fraud subpoena.

19 So, but from a legal point of view, all
20 decisions or all subpoenas which are not recognized and
21 enforceable by national law, legally, they mean nothing.
22 You can accept it if you like it, you can say I accept
23 this subpoena, I don't accept this, but from a legal
24 standpoint, that's a problem of, as I said, recognition
25 enforcement of foreign decisions. That's pretty much

1 the same in all legal systems in the world.

2 So, you can say certainly in your contracts with
3 your client, if you are able to establish a contractual
4 relationship with them, if we got a subpoena and/or if
5 we get this from a foreign agency, we do that, you know,
6 we would do that action, but if you don't establish it
7 in a contractual relationship, foreign decision,
8 whatever is legal, if it's right or wrong, if it's legal
9 it doesn't mean anything.

10 That's a major problem. And if you go through
11 this, which you can find in different treaties how this
12 is going to happen, the acceptance and recognition of
13 foreign decisions, if you go through that whole process,
14 which is very complicated, they have to be translated
15 and run through three desks and then it takes probably a
16 half a year, at least, to get something then translated
17 and then being enforceable in another legal system. So,
18 this is just practical that it's the way things are.
19 And if we find a formal way to solve that problem, I
20 would certainly be much more happy with that.

21 MS. MITHAL: Thank you, Phillip.

22 Kathryn?

23 MS. KLEIMAN: As a user, I have to say I'm
24 reassured by what I'm hearing from the different
25 countries, and the different registrars. There is a

1 real concern with the registrants and that contractual
2 relationship, which I think is important.

3 What I wanted to raise is that in the Internet
4 world, everything is kind of -- reciprocity is such an
5 important issue, and that as -- I can understand why you
6 would be asking foreign registrars to help with speed
7 and access, but domestically, where my domain name is
8 registered domestically, and were the local registrars
9 to give information on an informal basis to foreign
10 governments, I think we would just have exactly the same
11 problem that we're hearing the foreign registrars raise.

12 Because you're so -- you being the Federal Trade
13 Commission -- are so much on top of this problem. You
14 are very much at the forefront, I think, of the fraud
15 enforcement that's taken place. But others will follow
16 you, and you are in the position to kind of set the
17 model. And I think what you are hearing is that the
18 model should be one of process, verification, legitimate
19 reasons, as well as speed.

20 So, you get to build the model. And I actually
21 wanted to thank AT&T for setting the gold standard in
22 this area. In the 1950s and 60s, the U.S. Government
23 went to AT&T, as I understand the story, and said we
24 want informal access to contents of telephone calls, and
25 AT&T said, privacy and process are the right answers,

1 that's what protects our subscribers. And we had to
2 pass laws, considerable laws about subpoenas and court
3 orders and under what circumstances that information
4 would be given up, and you're in the process of building
5 the new model. So, good luck.

6 MS. MITHAL: Thanks.

7 Dan?

8 MR. SALSBURG: We don't have years, and that's
9 the problem, and I think that's why I'm thrilled that
10 you are all here. We all know that it does take years
11 to develop these government-to-government models for how
12 to do this. The problem we have is that in the mean
13 time before these things are formalized, consumers are
14 going to lose a tremendous amount of money from becoming
15 victims of frauds.

16 And that's my problem here in the FTC, not
17 necessarily yours in the CCTLDs, but you have a related
18 problem, and that problem is that -- and we've seen this
19 in other mediums of commerce, if it turns out that U.S.
20 law enforcement can't do its job to protect consumers in
21 a certain medium, that medium runs the risk of becoming
22 a haven for pariahs, and for fraudsters, and in which
23 case the medium fails.

24 And so I guess the warning out there is be
25 careful, you don't want to have your CCTLD go the route

1 of certain other mediums of commerce that have just
2 become known as where you get your psychic reading or
3 your chit-chat with a supposedly naked lady. That's not
4 what you want to have happen with your CCTLDs.

5 So, how do we deal with this? Well, in my mind,
6 really the only way to deal with this issue is to, yes,
7 formalize relationships, but they have to be formalized
8 at the FTC to registrar level. That's the only way
9 we're going to be able to achieve protecting consumers
10 and also creating the framework for ensuring, you know,
11 we deal with these other issues of the privacy issues in
12 a manner that's appropriate, and I think here at the
13 FTC, we feel that we're pretty -- we're pretty savvy to
14 issues of consumer privacy. But, you know, we can deal
15 with those issues, and also ensure that consumers in
16 America are protected, and also that the CCTLD continue
17 to function and grow.

18 MS. MITHAL: Thanks, Dan.

19 Paul, I will give you the last word on this and
20 then I had another question that I wanted to raise.

21 MR. KANE: I will try and be very brief. We are
22 all very familiar with caveat emptor, buyer beware.
23 What I found very interesting from yesterday's debate
24 where we were fortunate to have Mark MacCarthy here from
25 Visa. One of the questions I raised yesterday was,

1 wouldn't it be better to prevent the fraud or the
2 fraudsters from actually being able to transact.

3 We're in an age of electronic communications,
4 and it's possible through various techniques for banks
5 to notify registrars within milliseconds whether or not
6 a card, a credit card, facilitating the purchase of a
7 domain, is indeed valid.

8 Privately, or after the debate, the gentleman
9 very kindly said, such technology may exist, but banks
10 work at different speeds. What he was really trying to
11 say is it's different costs. If you think there are, as
12 we learned yesterday, somewhere in the region of 150
13 million chargebacks by U.S. and Canadian banks each
14 year, and banks charge between \$50 and \$25 U.S. dollars
15 per chargeback, there's one hell of a lot of money at
16 stake if banks try and tighten up the abusive use of
17 credit cards. They lose money.

18 We learned yesterday that their exposure rate,
19 the bank's exposure rate, has fallen from ten cents in
20 \$100 to seven cents in \$100. It is the merchants, it is
21 the registrars who actually carry that. They get a
22 refund.

23 One of the things I think the FTC could try and
24 do, which would stem this problem, is to try and
25 encourage this partnership to extend a bit more. Where

1 the banking system can actually share information with
2 registrars, which will give you guys and registrars the
3 heads-up that a fraud could be taking place, they're
4 registering a domain name. They haven't paid for it,
5 that's part of the gripe.

6 Where a registration takes place that hasn't
7 been paid for, it's almost tantamount to fraud anyway.
8 So, prior to registration there's a requirement for
9 payment. So banks would know if it was going to be a
10 fraudulent payment, the registrar would know and he
11 wouldn't activate the domain name. So, it's quite
12 simple.

13 Also in another conversation we were talking
14 about international fraud, we're talking about
15 cross-border fraud here. Another interesting statistic,
16 it takes between 10 and 12 days for the international
17 credit card service to exchange information
18 internationally. A specific example, I am from the UK
19 and my card is stolen here in the U.S. I will ring up
20 my bank in the UK and advise them that my card has been
21 stolen. It will be 10 to 12 days before my card in the
22 U.S. is deactivated.

23 Now, during that time, a registration could be
24 made, a fraudulent transaction facilitated, and for ten
25 days the guys could be defrauding consumers.

1 So, it's really in the day of electronic
2 communications, is to try and get the whole
3 public/private partnership together such that fraud can
4 be prevented at source and registrars aren't exposed to
5 liability, consumers aren't exposed to liability, and
6 working, as I mentioned yesterday, with consumer
7 associations, FTC and the like, internationally, would
8 actually really make a difference, but I think the banks
9 are the key, and for obvious reasons, they aren't that
10 keen to drop their chargeback routine in a hurry.

11 MS. MITHAL: Thanks, Paul.

12 It seems like there's a lot of consensus about
13 the fact that law enforcement should get speedy access
14 to information, but there are some constraints, and
15 people have raised various constraints, and I'm
16 wondering if we can talk about a way to move forward on
17 these issues. People have mentioned the idea of
18 creating government contact lists. You know, is that
19 something maybe the OECD could do, or another body,
20 could this discussion take place within the government
21 advisory committee to ICANN? You know, I think law
22 enforcement certainly would be interested in talking
23 about these efficiencies further.

24 So, I wanted to get other people's thoughts on
25 that. Michael, can I ask you about the OECD?

1 MR. DONOHUE: Well, the other side of the
2 cross-border fraud coin is government-to-government
3 cooperation, and we've been working pretty hard on that
4 at the OECD. And it's pretty hard going. We find that
5 a lot of our -- the enforcement regimes that are set up
6 in the other countries don't look like each other always
7 and can't always take to one another for many of the
8 same reasons that the data privacy rules as well.

9 So, I think looking to the OECD to help
10 formalize this role may not be -- it may not be
11 addressed with the speed concerns that have been
12 expressed earlier.

13 On the other hand, doing things like finding out
14 contact points, that's maybe not quite so hard. We have
15 a disadvantage of only having 30 countries that
16 participate in the OECD. Although that's not
17 necessarily new information, I would throw that out.

18 MS. MITHAL: Anybody else, ideas for moving
19 forward?

20 Phillip?

21 MR. GRABANSEE: Again, I can only advocate,
22 which is also a formal relationship, if the FTC would
23 establish relationship with the consumers. Associations
24 in various countries, however they might be organized,
25 and establish a network working together with them and

1 identifying fraud or potential fraud, informing the
2 partner organization, however this might be organized,
3 and the organization in the country where the domain
4 name is located, takes whatever action which is in the
5 legal system in the country possible.

6 For example in Germany, if you have the consumer
7 associations, if you see there's going to be some fraud
8 coming from a website, which is located in Germany, or
9 domain name, you inform German consumer associations and
10 they go, for example, to civil court and get a temporary
11 injunction which and then the temporary injunction is
12 properly served and there's no concern that also for the
13 registrar who gets a German temporary injunction, he can
14 just follow the legal procedure and I think that's my
15 suggestion for the time being.

16 Before, as we mentioned, we don't have years,
17 you know, but we could do something. The problem is
18 probably that the countries where domain names will be
19 located where people commit fraud, they will not have a
20 very established system of consumer protection,
21 organizations that will probably not have a very
22 effective legal system because that's why people hosted
23 and keeps the domain names in those countries, but
24 that's a situation that will always help, because those
25 other countries will probably be most difficult to agree

1 on mutual treaties, because that's how they live and how
2 they make their money, through those kind of people.

3 So, there is no clear solution to that, but
4 working together with the agencies in the countries
5 where they exist could certainly help.

6 MS. MITHAL: Thank you, Phillip.

7 Marilyn?

8 MS. CADE: I am at the risk of being somewhat
9 controversial, I'm going to sort of suggest two things.
10 One is I do think that the GAC, the Government Advisory
11 Committee, at ICANN offers a new opportunity, because
12 there's a new chair, there's a secretariat, and I think
13 that it might be possible to explore the creation of a
14 group of interested counterparts to the FTC to begin a
15 dialogue about how to begin to move forward.

16 The second idea that I would say, at least we
17 all ought to begin to have some beginning exploration on
18 it. It's not a perfect idea by any means, but in the
19 U.S., in the enactment of the Digital Millennium
20 Copyright Act, a compromise was struck between the
21 contact community and the ISPs and there is a procedure
22 for an expedited subpoena, an enforcement and takedown
23 procedure. And that is not a slam dunk.

24 The content owner, I'm the ISP, so let me just
25 make sure which hat I'm wearing now, I get the

1 subpoena. The content owner goes to court, there's a
2 form that is maintained by the copyright office. They
3 have to get a clerk of the court to stamp it. They have
4 to present prima facie evidence there as a violation and
5 the ISP is able to take the offensive content down based
6 on the subpoena. That then allows the content owner to
7 pursue other legal means.

8 I know this is probably not a popular idea, but
9 in the situations where there's clear evidence of fraud,
10 and I am not thinking that this -- I don't take this
11 lightly, but where there's clear evidence of fraud or
12 there are other really serious problems, perhaps we
13 should begin to think about an administrative procedure
14 which has safeguards, and I do say that safeguards are
15 necessary.

16 I think it cannot be so simple that people would
17 just print a copy of the format and fill in their claim
18 and send it to the registrar. But in the case that I
19 told you about, AT&T-Global.Net, AT&T owns the trademark
20 AT&T, we can present the prime facie evidence that that
21 is our trademark, and I throw that out as an idea to
22 start thinking about realizing that there have to be
23 safeguards and there has to be respect for national law.

24 MS. MITHAL: Marilyn, I think that's a really
25 good segue into the final topic that we wanted to talk

1 about today, and that is the taking down of fraudulent
2 websites.

3 And, Dan, can I ask you again to outline the
4 problem.

5 MR. SALSBURG: Sure. Domestically in the U.S.,
6 when we sue a fraudulent operator of a website, one of
7 the key remedies we seek in a temporary restraining
8 order is to have the registrar pull the website down.
9 That way there can't be any further fraud.

10 Clearly this remedy doesn't work as well. Okay,
11 to be honest, it doesn't work when dealing with foreign
12 registrars. An example of this is we filed a case a
13 little over a year ago against a man named John
14 Zucharini who was running a couple of thousand websites
15 that were all slight misspellings of popular names, you
16 know, National Rent-a-Cab sort of thing, instead of
17 National Rent-a-Car. And these websites, a large number
18 of them, were registered abroad.

19 We got a takedown order from the U.S. court, we
20 sent copies of it to the foreign registrars, nothing
21 happened. You know, there needs to be some way of
22 effectuating these sorts of takedown orders, because
23 from our perspective, whether or not a website is based
24 in the United States or abroad, it's still having an
25 impact on U.S. consumers.

1 One kind of interesting wrinkle to this is the
2 consumer can even think that he or she is going to a
3 .com, but be automatically redirected to a CCTLD and
4 suddenly, you know, we're in the arena of having to
5 figure out how to serve this order on a registrar of a
6 CCTLD.

7 So, that's kind of the problem that we're
8 having.

9 MS. MITHAL: And I think that this issue raises
10 some of the same issues that we just talked about in
11 terms of formal cooperation versus informal cooperation.
12 But I'm wondering if it's a little bit different in that
13 do registrars have terms of service agreements with
14 registrants prohibiting use of websites for fraud, and
15 could that be used as a basis to take down websites.

16 So, let me start with Willie and then I'll go to
17 Mike and then Wayne.

18 MR. BLACK: Before you went on to this topic I
19 was going to follow up on what was being said. In our
20 terms and conditions, and I have to say when we set up
21 Nominet, we focused very much on the terms and
22 conditions and the relationship between the registrant
23 members who are agents for the registrant, and us, and
24 so there are three contracts basically there that you
25 have to think about.

1 And under our terms and conditions, our contract
2 says that we may transfer, suspend, cancel or amend,
3 I've never actually tried to amend a domain name, I
4 suppose that's change it to another registrant, but
5 that's just transfer, upon receiving a copy of a
6 perfected order of a court of competent jurisdiction
7 requiring such action or where the retention of a domain
8 name by you, that's the registrant, would be
9 inconsistent with the terms of the perfected order
10 received by us.

11 So, it is a legal term, but the question is what
12 is a perfected order? Now, we know what a perfected
13 order is, my lawyer will know what a UK court stamps on
14 a document and should be able to verify that. But,
15 again, with all due respect, I don't think we would
16 really know whether it was a proper stamp of a U.S.
17 court or a Canadian court or an Australian court. And
18 that gets back to now there are means of mutual
19 recognizing court orders, but we think that we probably
20 would in a case-by-case basis, it depends how many of
21 these we're going to get. If we're going to get ten a
22 day, then we're talking back really to the economics of
23 how you can transfer domain names. And if that's the
24 world in that state, then we may have to face up to
25 that.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

1 But assuming that it was occasionally a request,
2 then I think we would look on a case-by-case basis, and
3 maybe we would actually investigate whether the stamp
4 and the crest and everything that we're seeing on this
5 order that you're sending us is really something that we
6 can say, yes, that is a U.S. court. Maybe we would
7 phone up somebody that we know and get some
8 confirmation, does it really look like that. You know,
9 we've got relationships with U.S. lawyers and so maybe
10 we would phone up our colleagues in DC and say, you
11 know, can you fax them a copy and is that really
12 genuine.

13 So, we can do it on a case-by-case basis, but I
14 think it would be much more difficult outside of the
15 commonwealth companies and maybe outside the EU. So,
16 once you start to get to some of the other parts of the
17 world, I think it's going to be very difficult. But I
18 believe that we would act on a court order if we could
19 just verify that it was perfected in some way without
20 necessarily going through the mutual court system where
21 you have to apply for an arm's-length judgment or
22 something.

23 MS. MITHAL: Mike?

24 MR. PALAGE: Regarding trying to work on taking
25 down websites, there was a case that just came out, what

1 is it, about a week or so ago, involving Verisign.
2 Where what happened was it was a trademark owner,
3 brought an action under the ACPA, and the court order
4 basically said take down the website. The domain name
5 registrant went to Korea, got a court in Korea to say,
6 no, don't do that.

7 So then the trademark owner went back to the
8 court here in the U.S. and said, well, we have two
9 competing court orders, and, you know, since we
10 initiated our court proceeding first, the U.S. would
11 trump the Korean court order, and basically in that
12 second proceeding, the court said, Verisign registry,
13 take it down.

14 So, you're very lucky, being very near to the
15 Eastern District of Virginia, that you have a
16 substantial chunk of the domain name .space, .com, .org,
17 .net, .us, .bus, a lot of the registries have
18 significant contacts in this area.

19 Now, let me put one little caveat here. Be
20 careful what you ask for, because you may get it. Now,
21 let's just take the Zucharini case. Let's just suppose
22 you say, dear Verisign, take down these names, assuming
23 they're, say, common net names. What's going to happen
24 is as Willie and everybody said, the bad guys are pretty
25 smart. And what's going to happen is, as soon as you

1 take down the domain name, the domain name is probably
2 going to be reregistered after it gets through the
3 redemption grace period or whatever procedure it must go
4 through, and it's probably going to be reregistered in,
5 you know, John Doe or some other name which would then
6 potentially put the FTC back on -- back to square one,
7 if you will, of trying to take down the person.

8 So, in fact, what you may want to do is when
9 asking if you were to try to say, dear registrar, do X
10 or do Y, you may just say please take out the DNS and
11 sort of let the name expire its natural, if you will,
12 death. Because again, one of the things we're concerned
13 about here is unfunded mandates, and obviously
14 registries and registrars are in the business of making
15 money, and you can't go to a registry or a registrar,
16 take a name away or don't allow it to be reregistered by
17 anyone. It's rather difficult.

18 And as I said, you know, we're trying to talk
19 about theoretical and practical, but these are some of
20 the practical things that you need to know about in
21 trying to tackle the bad guys, and how if you do work,
22 if you do have this public/private sector cooperation, I
23 think you'll sort of find ways of beating the bad guys
24 and helping consumers and businesses.

25 MS. MITHAL: Wayne?

1 MR. MacLAURIN: Certainly for our part, again,
2 we do things on a case-by-case basis. Taking down a
3 domain is a whole lot easier than us turning over
4 information. Because our terms of service also clearly
5 state that we can -- we will do that, we will take it
6 down and transfer it for a reasonable court of
7 jurisdiction.

8 We refer everything to our lawyers, who make
9 that determination for us, and we are fortunate enough
10 to have a law firm that does have locations all over the
11 place.

12 So, for us, yeah, great. Can we take down a
13 website, or put it on hold? That's much easier than
14 turning over customer information or credit card history
15 or something like that.

16 MS. MITHAL: Phillip?

17 MR. GRABANSEE: Again, I want to make clear that
18 it's certainly possible to solve this problem, including
19 it in the terms and conditions, but that's taking a lot
20 of burden on the registrars, especially the small one,
21 because it's extremely complex to create such terms and
22 conditions, and every legal system.

23 It's easy for Willie and his company with four
24 million registrants to establish a rule like this one
25 time and then enforce it, than for the smaller or medium

1 size registrar. And because it's very time consuming
2 and it's also extremely complex because the whole
3 system, a registrar, registrant, registry relationship,
4 especially in the CCTLD domain space, it's really very
5 much space on the Anglo-Saxon legal thought. So, it is
6 possible to include it, but I have to, you know, as a
7 registrar and consistency representative, wear that hat.
8 It puts the burden again very much on the registrar,
9 which already operates in a very difficult environment.
10 But probably he has to carry that maybe.

11 MS. MITHAL: Thanks.

12 Okay, Willie, last point, and then I think we'll
13 take the questions.

14 MR. BLACK: Just a very quick one. Just
15 remember, of course, that us removing a domain name
16 registration, or even suspending it, which is what we
17 would say is taking away the servers and so it still
18 remains in the register, let's say until a court finally
19 makes a determination, we're quite happy to do that,
20 although if it takes a long time and the domain would
21 normally expire during that time, it gives us a little
22 issue of whether to keep it suspended beyond the time
23 that we would have been paid for the renewal.

24 But just taking it down does not remove the
25 website. We're not talking here about an order against

1 the host of the web of the material. It's still there,
2 and if they've got the right key words and everything
3 and the Googles pick it up, the people will still find
4 that fraudulent website, even without a domain name.
5 So, it's not the perfect solution just to get rid of the
6 infringing website.

7 MS. MITHAL: Thank you.

8 Last word, Kathy, and then we'll wrap up and
9 take the questions.

10 MS. KLEIMAN: I get the last word? Wow.

11 Dan, I just wanted to reiterate something that
12 I've raised already, which is that when you say that
13 fraud is being committed on U.S. citizens by people
14 operating in foreign countries and therefore you want to
15 reach them, that sends a chill up my spine, as I know
16 that foreign governments are going to want to reach U.S.
17 citizens who are doing things against their laws, some
18 of which we consider to be completely legitimate. The
19 whole extra territorial reach of the Internet just
20 raises such huge problems.

21 The domain name websites that you are trying to
22 take down are speech, and so the more process -- and
23 commercial speech is entitled to First Amendment
24 protection in the U.S., not as high as political speech,
25 but it's entitled to it. So, the more process that

1 surrounds all of this, from the user perspective, even
2 though it takes time and we have to expedite it, from
3 the user perspective, the more process that surrounds it
4 protects speech of all sorts and it sounds like we're
5 hearing that it protects the registrars and registries
6 as well.

7 MS. MITHAL: I guess I think I'll give myself
8 the last word and just respond to Kathy. I think that's
9 a very good point. And I think one of the reasons why
10 we wanted to talk about cross-border fraud and fraud in
11 general was that we were hoping that that was at least a
12 common denominator that fraud is against the law in all
13 countries. And if we can kind of agree to that and then
14 only talk about fraud at this particular workshop, I
15 realize it raises all the issues that you raised, but
16 for the purposes of this discussion, I think that's why
17 we limited it to fraud.

18 So, we heard a couple of ideas during this half
19 of the panel about moving forward on this. We talked
20 about getting the OECD or another body to do government
21 contact points that can facilitate information sharing
22 and cooperation in this area. We talked about possible
23 further GAC work. Marilyn mentioned an idea of notice
24 and something similar to notice and takedown with lots
25 of procedural protections, and I think those are all

1 issues that we should continue to consider.

2 So, with that, I would like to take any
3 questions from the audience? Why don't we start in the
4 back of the room and work our way forward.

5 ELANA BOITMAN: Hi, I had a
6 practical question for Marilyn. In the AT&T case, it
7 sounds like the name continued to be registered and you
8 were dealing with just the web hosting company, which
9 was an imperfect solution because they could easily go
10 to another web hosting company, et cetera. Had you
11 reached out to the registrar? What sort of responses
12 did you get about getting the name taken down?

13 MS. CADE: Registrars vary in their response.
14 That would be only one of the many incidents I could
15 share with this audience. Famous well-known
16 brandholders seem to be sticky, that is everyone wants
17 to misuse their brand. And credit card fraud seems to
18 be a real serious and growing problem for all of us.

19 The registrars vary. We typically would -- this
20 happened on a weekend, began at 6:00 on a Friday night.
21 We do take all the legal action that we can, and
22 eventually we were able to get a temporary restraining
23 order. We were able to identify, we had to hire a
24 private detective in order to identify the perpetrator.
25 And it takes us time, just as it did law enforcement, to

1 identify the person who was actually, and then we of
2 course found out that he, in fact, was in another
3 country.

4 MS. MITHAL: The gentleman in the tan jacket.

5 UNIDENTIFIED MALE SPEAKER: Just a thought, has
6 FTC explored a relationship with INTERPOL, as we know
7 INTERPOL is present in all the countries and that might
8 be something to leverage off getting information that
9 you require?

10 MS. MITHAL: I can take a crack at that. I
11 think one of the things that makes the FTC unique is
12 that we are a civil law enforcement agency and we
13 certainly do reach out to criminal agencies, but I think
14 sometimes the cooperation in the criminal area, the
15 agreements that there are, the MLATs, you know, the
16 INTERPOL mechanisms that we can't take advantage of a
17 lot of them because we are a civil law enforcement
18 agency.

19 But that being said, we do have contacts there
20 and we are trying to build more relationships with
21 criminal agencies around the world.

22 Rick?

23 RICK WESSON: I wanted to talk about a couple of
24 things. First of all, when you --

25 MS. MITHAL: Rick, if you could limit it to one

1 question, I think we had other people who wanted to ask
2 questions, too.

3 MR. WESSON: Okay, I'll just do one. I had several.

4 MS. MITHAL: We'll get back to you if we have
5 time.

6 MR. WESSON: It's all right. First of all, the cost
7 of providing services was something that was discussed.
8 The cost of trying to identify a domain name is accurate
9 or not, which is something that you guys have encouraged
10 registrars to do, and I would just like to point out
11 that the financial community, NACHA, the credit card
12 processors, only verify a house number and a zip code in
13 one, potentially two, countries. The amount of dollars
14 going through those transactions is orders of magnitude
15 higher than the entire domain registration market.

16 And I really wanted to understand why that the
17 FTC was encouraging registrars to provide this service,
18 that the registrars are a very small community, not
19 nearly as well funded, don't have locations in the
20 number of countries that the credit card processing do,
21 nor the financial resources, and asking us to do
22 something that is orders of magnitude more complicated
23 and more costly than what financial institutions do.

24 And what I wanted to propose is that if we are
25 working cooperatively, that it's the relationship

1 between the merchant and the credit card processor, as
2 Paul pointed out earlier, where this could be more
3 effective and handle more of the fraud, killing two
4 birds, effectively, with one stone.

5 MR. SALSBURG: Let me take a crack at that. I
6 think we're dealing with different types of fraud when
7 you're talking about credit card fraud and the fraud
8 that you see in whois registrations. What we've found
9 in our Internet cases is that the whois data serves as
10 the building block of our investigation. If that data
11 is inaccurate, we have a burdensome time protecting
12 consumers at all. We recognize that credit card fraud
13 is awful, it's terrible for consumers, it's terrible for
14 the merchant banks, for merchants, but from an
15 investigative standpoint, whois data is a key.

16 MR. WESSON: May I ask a clarifying question?

17 MS. MITHAL: Sure.

18 MR. WESSON: Yes, could you tell us how much the
19 dollar amount of fraud that's committed from Internet
20 fraudulent domain names and compare and contrast that
21 with the other financial institutions?

22 MR. SALSBURG: Do you work with that?

23 MS. MITHAL: I mean, we can talk about some
24 statistics on Internet fraud, we just released some
25 statistics yesterday and I would actually encourage you

1 to go through that and we can talk about that a little
2 bit more later.

3 RICK: So you don't know the answer?

4 MS. MITHAL: I actually don't know the answer.

5 MR. KANE: Could I just follow up on Dan very
6 briefly?

7 MS. MITHAL: Sure.

8 MR. KANE: Dan, I think the point we're trying
9 to make is if the name is not paid for, they shouldn't
10 be in the whois anyway. We're a believer, I think the
11 registrar community, and the CCTLD community I believe
12 is, in having the whois publicly available. It's good
13 for consumer confidence, it's good for resulting
14 technical problems, it's good to have whois publicly
15 available. But if the bad guys are using credit cards
16 fraudulently to purchase the web space, to purchase the
17 domain name, to do all the stuff, if we can stop that,
18 nip it in the bud, they'll never get on and they can
19 never commit their crime. That's --

20 MR. BLACK: Please, please, yesterday we had
21 somebody saying that the fraudsters in Canada spent a
22 million dollars on phone bills. They're not going to
23 worry about paying \$50 for a domain name. They will pay
24 for it if they're genuine crooks, I mean if I can say
25 that. You know, they're actually going to be prepared

1 to go to a certain amount of genuine expense to rip off
2 100 times that. So --

3 MR. KANE: In which case you've nailed them,
4 because you've got their address.

5 MS. MITHAL: Can we continue to have questions
6 from the audience?

7 MR. CONNELLY: Thank you, I'm Robert Connelly
8 from PSI USA and PSI Japan. This conference has focused
9 upon cases in which consumers have been defrauded. I
10 would like to call your attention that the majority of
11 ICANN accredited domain name registrars are small
12 businessmen, or small businesspersons, some even IRS
13 section S, perhaps even sole proprietorship. None of us
14 is a Western Union!

15 These small businesspersons who have invested
16 heavily in their enterprises, most are honest,
17 hard-working, bright citizens of their various
18 jurisdictions.

19 They, too, are being defrauded.

20 Fraud may damage many persons all along the
21 supply line. Will this conference agree to conclude
22 that fraud is wrong, regardless of who are the
23 "suckees?"

24 My text for the secretariat.

25 MS. MITHAL: I think we had a question in the

1 back, Commissioner Bhojani.

2 MR. BHOJANI: Thank you. Sitesh Bhojani from
3 ACCC Australia. Dan mentioned earlier that one of the
4 problems with law enforcement was to have websites shut
5 down. Might I add that one of the other developments
6 we're making as law enforcement agencies is also to try
7 to get corrective measures on websites, just as you have
8 corrective ads in newspapers or radio ads and so forth
9 to help educate the community. One of the other
10 objectives law enforcement agencies are looking at is
11 getting corrective messages on commercial websites and
12 my question is directed to the registrar community.

13 Dan's question was about recognizing court
14 orders, especially from foreign jurisdictions, ordering
15 or requiring a website to be shut down. Would you have
16 a different view if it was a court order that required
17 you to transfer the domain name to a law enforcement
18 agency from a foreign jurisdiction?

19 Let me give you a specific example, if the ACCC
20 wrote you a letter, tried to verify who we were, showed
21 that we were a genuine law enforcement agency and said
22 that we wanted that domain name transferred into our
23 name, what would be the response from the registrars?

24 MS. MITHAL: Mike, do you want to take a crack
25 at it?

1 MR. PALAGE: Let me. If you're going to -- I
2 want to be real careful here. I would say, again, if we
3 had -- I think most registrars, if you are able to
4 verify that it was -- that you had a judgment from a
5 court of competent jurisdiction, and I guess here is the
6 most important caveat, that you were willing to pay for
7 the service, i.e., the domain name registration, which
8 as I said, you know, we're rather competitive and we
9 offer very good prices.

10 The cost of maintaining a registration to do the
11 corrective advertisement actually would probably be from
12 a cost benefit analysis, very -- a good return on
13 investment, because again, I think one of the things
14 that happens, and a lot of trademark owners have made
15 this mistake, where they'll file a UDRP, and they'll ask
16 for a cancellation instead of transfer, and as soon as
17 they prevail after expending several thousand dollars,
18 the UDRP will be enforced, the domain name is cancelled
19 and milliseconds later the name is registered by the bad
20 guy again.

21 So, I think part of -- as I said, I think what
22 you're saying about corrective advertising, you are
23 thinking outside the box, and staying ahead of the bad
24 guy. And as I said, if you're willing to pay registrars
25 and registries for their services, I think that that's

1 an excellent opportunity for cooperative venture.

2 MS. MITHAL: Phillip, did you have your tent up?

3 MR. GRABANSEE: No.

4 MS. MITHAL: Okay. In the front, Susan Grant?

5 I think this will be the last question, and then our
6 bureau director is here.

7 MS. GRANT: First of all, I am from the National
8 Consumers League and we're against fraud perpetrated
9 against anyone, businesses or consumers, and I do think
10 that banks, credit card associations and credit bureaus
11 could make information more readily available to help
12 you, and we would certainly support that.

13 I'm concerned about consumers' perceptions of
14 domain names. I was talking to a college class earlier
15 this week and asked them how they would identify a
16 website providing information about health as a
17 legitimate objective source of information, and one of
18 the first answers was, well, we would look to see
19 whether it was a .org or a .gov, but it seems to me that
20 there's not really any screening to make sure that
21 entities are who they are.

22 And then, there's the whole country domain name
23 now. There's something up right now that I think has a
24 name like ConsumerProtectionAgency.US, which is of
25 concern because it has the potential to deceive not only

1 U.S. consumers, but foreign consumers who may be trying
2 to contact U.S. Government with a problem, and this is,
3 in fact, a for-profit operation. So, I would like some
4 comment from the registrars about this.

5 MS. MITHAL: Anybody want to respond?

6 MS. CADE: Actually, I'm not a registrar, but
7 I'll take a crack at the first one. One of the
8 decisions that ICANN made when it introduced what is
9 called the proof of concept around the new GTLDs was to
10 introduce sponsored GTLDs with the idea that in order to
11 register in that GTLD, you had to meet certain criteria.
12 So in order to register for a museum you have to be a
13 museum and you have to present your credentials. And in
14 order to register in .aero, you have to be affiliated
15 with the aeronautics industry, et cetera.

16 I think one of the questions that is still being
17 debated and the evaluation that's going on is is that a
18 good way to expand the name space, and does it bring
19 some relationship between the name that is between the
20 TLD and the entities who are registering in it.

21 Beyond that, most of the TLDs are -- that are
22 available -- are open in one way or another and the
23 criteria for that is really not in the hands of the
24 registry or the registrar, but is set by ICANN policy.

25 MR. PALAGE: Okay, a couple of things. First,

1 with the .US, that is operated outside of the ICANN
2 regime, that is a CCTLD, and you have -- you're
3 fortunate enough two rows behind you is Jeff Newman from
4 Newstar, the registry administer for .US, so you may
5 want to contact him, and as I said, myself being a
6 policy member of the .US Policy Council, the U.S.
7 Government, I think, does have an interest, I mean, they
8 do have certain safeguards regarding trying to maintain
9 the space in a productive manner, and as I said, that's
10 something you definitely want to try to communicate.

11 Getting back to what registrars could do, I
12 think Bob during his statement really hit the nail on
13 the head that there are a lot of small to mid-size
14 registrars. If you look at it from a numbers
15 standpoint, let's just say there are 30 million generic
16 TLDs in the name space. If you look at the top 20, the
17 20th has 200,000 registrations, so the other 140
18 generally are dealing with thousands. And, again, these
19 are small to mid-sized businesses that are not in the
20 business to be a content policemen.

21 I work with a number of registrars that get
22 calls that say, well, this is child pornography or this
23 is that. You know, again, and it's rather difficult.
24 You know, again, most registrars, I think, are
25 responsive, they try to work, you know, with law

1 enforcement or they do try to respond to most valid
2 queries, but I don't think that they are in a situation
3 to take down ConsumerProtection.US, you know, again,
4 that's sort of where you need to work with your
5 counterparts here, you know, the people at the FTC to
6 try and identify something and take it down that way.

7 So, I think that would probably be the best
8 registrar situation or best generic registrar response.
9 We're not content police.

10 MS. MITHAL: Okay. Kathy?

11 MS. KLEIMAN: I think the college students have
12 a real challenge and if they understood the difference
13 between .org and .gov, they're doing pretty well. The
14 .gov sites are -- I mean, that would be a place to go.
15 That's not an open GTLD, that's the U.S. Federal
16 Government. They understand, they're beginning to
17 understand the differentiation.

18 But this is the big question, one of the big
19 questions for users on the 'net is, whose news website
20 do you trust, where are you getting your news, where are
21 you getting your health. We can't ask ICANN or the
22 registrars of the registry to be the speech police.

23 Part of the wonder of the 'net is that everyone
24 can participate. People are going to have to learn
25 where to get -- this is where third parties, people are

1 going to come in and tell us who's speaking, but please
2 don't ask ICANN or the registrars or registries to do
3 that kind of speech policing. It's not fair and it
4 ultimately isn't right.

5 MS. MITHAL: Well, with that, we will conclude
6 that panel on cooperation between enforcement agencies
7 and registrars and registries, and I want to thank
8 everybody, particularly those people who traveled from
9 far away to be here, and I want to thank everybody for a
10 very lively and interesting panel.

11 (Applause.)

12 MS. MITHAL: Now I would just like to introduce
13 Howard Beales, who is the Director of the Bureau of
14 Consumer Protection, and he will just make a few
15 concluding remarks about the conference.

16 MR. BEALES: I want to thank everybody for
17 coming and for some very informative and very productive
18 discussions over the last few days. And I wanted to
19 especially thank all of you in light of our own very
20 cross-border problems where cold air from Canada met
21 warm air from the Gulf of Mexico and produced blizzard
22 '03. I want to thank Stacy Feuer and Tara Mikkilineni,
23 who are really the keys of putting this together and
24 doing so despite some pretty difficult conditions at the
25 end, particularly given the snow problems.

1 I want to encourage anybody who is interested to
2 submit comments in writing, if you didn't have a chance
3 to say something here, then send it to us in writing,
4 and we will, of course, we will of course consider that.
5 But I think it's, you know, it's particularly useful
6 since there may have been people who wanted to be here
7 and couldn't make it.

8 I did want to highlight a few key points I think
9 that come out of the workshop and that are areas for
10 further work together. First is I think a very general
11 recognition that cross-border fraud is harming consumers
12 and harming legitimate businesses. It imposes costs in
13 terms of dollars, it imposes costs in terms of the
14 resources that we devote to fighting fraud as economists
15 are fond of saying, part of the cost of crime is what we
16 invest in locks. And it imposes cost in loss of
17 consumer confidence and in damage to reputation.

18 Second, there's obviously a role for vigorous
19 law enforcement from the FTC and from criminal law
20 enforcement authorities, and that's help, but more needs
21 to be done on a systemic basis to try to curb the
22 problems rather than rely simply on after-the-fact
23 enforcement.

24 Third, I think it's been clear that the private
25 sector is willing to help and has acknowledged the

1 importance of speed in dealing with cross-border fraud.
2 It moves quickly and we have to, too, if we're going to
3 make any difference.

4 Fourth, I think the keys to successful
5 public/private partnerships are concrete objectives that
6 we want to accomplish in clear, well-understood
7 divisions of responsibilities. We need to make best use
8 of the information and the resources that we each bring
9 to the table. We don't want to ask private sector
10 businesses to become law enforcers, or to assume broad,
11 unfunded mandates, but we do want to ask you to
12 contribute the tools and the information that you have
13 to what really is a common cause.

14 And I think a final key is working across
15 borders. For the FTC, pairing with consumer protection
16 law enforcement agencies in other countries, for the
17 private sector in working with affiliates abroad, so
18 that a public/private partnership really can work across
19 borders just like the fraud operators that we're trying
20 to pursue.

21 I think there's also some specific areas of
22 agreement that are applicable to all of the private
23 sector participants, and some industry-specific points
24 that I think are worth making. I think there's a
25 consensus that there's a need for some sort of broader

1 information sharing, that that's one thing we can
2 clearly do and as well as training and business and
3 consumer education. I think we can work on those
4 things.

5 In particular, I think government and private
6 sector can do a lot more to put in place mechanisms that
7 maximize the speed and timeliness of information
8 sharing, and that minimize confusion and delay. We can
9 appoint agency liaisons with private sector
10 organizations. We can put together resource lists of
11 private sector representatives who are working on
12 cross-border fraud and security issues. We can have law
13 enforcement work together to set up referral points for
14 information that's coming in from the private sector.
15 We can develop ways to identify the right agencies for
16 the private sector to contact and cooperate with in
17 particular matters. And to authenticate that you really
18 are dealing with somebody from that agency.

19 We certainly don't want our identity stolen. We
20 can use companies' internal communication systems to
21 share information about the latest frauds and about
22 enforcement needs. And we can set up training sessions
23 so that law enforcement understands the way that
24 business operates and the best ways to frame requests
25 for information, and so that companies understand the

1 way the FTC works in our civil law enforcement
2 investigations. You certainly don't want to find out by
3 being a target.

4 Turning to some of the specific industrial
5 areas, or business areas, in the financial sector, I
6 think there's a consensus that information from some of
7 the very sophisticated tracking and risk assessment
8 techniques and mechanisms that are already in place
9 would be valuable to the FTC. I'm certainly convinced.
10 I think that would be extremely useful for us to be able
11 to access, use, understand consistent with your needs.

12 And I think for payment systems, there's some
13 fairly clear agreement that some mechanisms that are
14 already widely used, such as fraud alerts that are
15 circulated by the credit card industry, can be expanded
16 to include the FTC and hopefully to facilitate reducing
17 the problem. And I think more consumer education,
18 including at the point of purchase, is something that
19 may also be helpful.

20 In particular, we would like to follow up on the
21 suggestion to look at ways to have industry analysts
22 work with law enforcement to analyze data we currently
23 have available. How can we make better use of the
24 complaint data we get to select targets, and that's
25 something where there's a lot of expertise in this room

1 that unfortunately doesn't work for the FTC.

2 For commercial mail receiving agencies, and for
3 courier services, I think expanded training for
4 operators and courier agents who deal directly with
5 consumers is something that could be a very useful tool.
6 In particular, I would like to thank FedEx and MBE for
7 their offers to follow up in this area. I think that's
8 something that would be quite useful.

9 And for ISPs and web hosting companies, I think
10 there was agreement that it's important to be able to
11 act quickly on information preservation requests, and to
12 consider whether we can find a way to pass on
13 preservation requests to the next organization in the
14 evidentiary chain. There's interest in using companies'
15 terms of services -- terms of service -- both to address
16 privacy concerns, and to stop websites that are
17 determined to be fraudulent. And I think there's some
18 interest in developing a vehicle for consumer protection
19 agencies in various countries to work cooperatively to
20 obtain information from companies that are outside of
21 their jurisdiction.

22 For domain registrars, in particular, I think I
23 heard some agreement, that there should be a way for
24 legitimate and verifiable law enforcement agencies to
25 get access to accurate whois data. I recognize that it

1 has some costs, but it's the essential first step in
2 knowing who it is that we're investigating and where to
3 go.

4 I think there should be streamlining of requests
5 for cooperation from law enforcement to domain
6 registrars and to registries. We should try to utilize
7 identifiable points of contact with you all, and with
8 law enforcement agencies around the world.

9 I think it's interesting that a concern cutting
10 across all the panels is the interface with privacy
11 laws. I think information sharing and information
12 utilization is a key to the fight against fraud. I
13 think we need to focus on the ways that information is
14 used, and there's some good uses of information, like
15 fighting fraud, where we should strive to not let
16 privacy regulations get in the way. And we may need to
17 work together to find ways to harmonize the need for
18 that greater flow of information, with privacy schemes
19 in various countries.

20 In summary, I think this workshop demonstrated
21 there's a very real and very important need for
22 public/private partnerships to combat cross-border
23 consumer fraud. There's a lot of details to be hammered
24 out, and a lot of issues that still need to be decided.
25 But I think this meeting put us one step closer to

1 creating ongoing and productive partnerships.

2 We look forward to continuing to work together
3 on the issues and the ideas that have been generated by
4 this workshop. And, again, I want to thank you for your
5 contributions of your time and your effort and your
6 attendance. Thank you all very much.

7 (Applause.)

8 (Whereupon, at 5:15 p.m., the workshop was
9 concluded.)

10 - - - - -

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25